

Front Cover

**(4) Defense Production of Government Reciprocal Discovery Request**

(A) Date: 14 September 2012

**(5) Government Motion to Compel Discovery (if any)**

(A) Filing: 28 September 2012

(B) Response: 3 October 2012

(C) Article 39(a): 15-19 October 2012

**(6) Defense Notice of Accused's Forum Selection and Notice of Pleas in Writing<sup>11</sup>**

**(7) Motions *in Limine* (Supplemental, Including any Classified Information)**

**j. Interim Pretrial Motions (22 October 2012 – 31 October 2012)**

(A) Filing: 22 October 2012

(B) Response: 26 October 2012

(C) Article 39(a): 31 October 2012

**(1) Updated Proposed Case Calendar**

**(2) Production of Compelled Discovery for Government Motion to Compel  
Discovery**

(A) Date: 22 October 2012

**k. Pretrial Motions (2 November 2012 – 30 November 2012)**

(A) Filing: 2 November 2012

(B) Response: 16 November 2012

(C) Article 39(a): 28-30 November 2012<sup>12</sup>

**(1) Pre-Qualify Government Experts**

**(2) Requests for Judicial Notice**

**(3) Supplemental Government Witness List<sup>13</sup>**

**l. Interim Pretrial Motions (7 December 2012 – 20 December 2012)**

(A) Filing: 7 December 2012

---

<sup>11</sup> If the accused selects a panel, the United States proposes the panel be notified no less than sixty days prior to trial, in order to coordinate for extended special duty and travel.

<sup>12</sup> The hearing is scheduled one week later than the default schedule due to the Thanksgiving holiday.

<sup>13</sup> The United States will submit a supplemental witness list based solely on any rulings from the government motion to compel discovery ruling and any disclosures by the defense after the 14 September 2012 witness list due date.

- (B) Response: 14 December 2012  
(C) Article 39(a): 19-20 December 2012

- (1) **Litigation Concerning MRE 505(h) and MRE 505(i)**<sup>14</sup>  
(A) Filing: 14 November 2012  
(B) Response: 27 November 2012<sup>15</sup>  
(C) Article 39(a): 19-20 December 2012

(2) **Updated Proposed Case Calendar (if necessary)**

**m. Pretrial Motions (14 December 2012 – 11 January 2013)**<sup>16</sup>

- (A) Filing: 14 December 2012  
(B) Response: 28 December 2012  
(C) Reply: 2 January 2013  
(D) Article 39(a): 9-11 January 2013

(1) **Any Additional Motion that does not have an Identified Deadline**

(2) **Grunden Hearing for All Classified Information**

- (3) **Voir Dire Questions, Flyer, Findings/Sentence Worksheet, All CMCOs**  
(A) Filing for Court Review: 2 January 2013  
(B) Article 39(a): 9-11 January 2013

**n. Trial by Members (18 January 2013 – 8 February 2013)**

- (A) Voir Dire: 18 January 2013  
(B) Trial: 21 January 2013-8 February 2013

  
ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

<sup>14</sup> This includes *in camera* proceedings for Defense Notice to Disclose Classified Information and/or the Government's Invocation of the Privilege for Merits and Sentencing Information. The United States estimates that any Court order to disclose classified information will likely require coordination with multiple federal organizations and roughly estimates forty-five to sixty days to aggressively coordinate a response across all equity holders.

<sup>15</sup> The adjusted date gives the Court additional time to review any discoverable material and was agreed to by the defense. The Government estimates the review will take no more than fifteen duty days to complete.

<sup>16</sup> There have been numerous unplanned motions submitted throughout the pre-trial process. The prosecution, therefore, anticipates that several pretrial motions will be filed under the "Any Additional Motion" timeframe.

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211 )

Prosecution Proposed  
Case Calendar  
Update

30 June 2012

1. The Court is currently scheduling Article 39(a) sessions with the following default schedule at the request of the parties: two weeks for parties to file motions; two weeks for parties to file responses; five days for parties to file replies; and one week for the Court to review all pleadings before the start of the motions hearing. The time for filing replies was added after the first Article 39(a) session on 15-16 March 2012 because the Court received reply briefs the day before that session, the parties desire to continue to file replies, and the Court requires time to consider them.
2. The Prosecution Proposed Case Calendar Update, dated 30 June 2012, is based upon the same assumptions listed in the Prosecution Proposed Case Calendar (AE I) and all Prosecution Proposed Case Calendar Updates and Supplements (including AE XX, XLV, XLVI, CXIII, CLI, and the Prosecution Proposed Case Calendar Updates, dated 22 June 2012 and 29 June 2012). To the extent these assumptions prove to be incorrect or too ambitious, the schedule will be correspondingly longer.
3. Scheduling dates and suspense dates are set forth below. The trial schedule will be reviewed and updated as necessary at each scheduled Article 39(a) session.
  - a. Immediate Action (21 February 2012 - 16 March 2012)
  - b. Legal Motions, excluding Evidentiary Issues (29 March 2012 - 26 April 2012)
  - c. Legal Motions (10 May 2012 - 8 June 2012)
  - d. Interim Pretrial Motions (2 June 2012 - 25 June 2012)
  - e. Pretrial Motions (7 June 2012 - 20 July 2012)
    - (A) Filing: 22 June 2012
    - (B) Response: 6 July 2012
    - (C) Reply: 11 July 2012
    - (D) Article 39(a): 16-20 July 2012

**(1) Defense Motion to Compel Discovery #2 (Department of State Material)<sup>1</sup>**

<sup>1</sup> See Appellate Exhibit (AE) CXLII. AE CXLVII changed the response date to 9 July 2012.



- (A) Filing: 7 June 2012
- (B) Response: 9 July 2012
- (C) Reply: 11 July 2012
- (D) Article 39(a): 16-20 July 2012

**(2) Government Initial Witness List**

- (A) Filing: 22 June 2012

**(3) Proposed Members Instructions for All Charged Offenses**

**(4) Witness Lists for Article 13**

- (A) Defense Witness Lists: 3 July 2012<sup>2</sup>
- (B) Government Objections (if any): 10 July 2012
- (C) Defense Motion to Compel (if any): 13 July 2012
- (D) Article 39(a): 16-20 July 2012

**(5) Preliminary Determinations on Admissibility**

**(6) Defense Motion to Dismiss All Charged Offenses under 18 U.S.C. 1030(a)(1) #2**

**(7) Maximum Punishment for Lesser Included Offenses**

**(8) Government Motion for Substitutions under MRE 505(g)(2) for FBI Impact Statement**

**(9) Government Motion for Modification of Court Order: Government Motion: Protective Order(s) dated 24 April 2012**

**(10) Supplemental Filings on Actual Damage on the Merits**

- (A) Filings: 21 June 2012

**(11) Proposed Questionnaires**

- (A) Defense Filing: 6 July 2012
- (B) Prosecution Response: 11 July 2012
- (C) Article 39(a): 16-20 July 2012<sup>3</sup>
- (D) Questionnaires to Detailed Members and Alternates: 24 July 2012
- (E) Suspense for Detailed Members and Alternates to Respond: 3 August 2012

**(12) Updated Proposed Case Calendar<sup>4</sup>**

- (A) Filing: N/A

---

<sup>2</sup> The United States moved the date from 6 July 2012 to 3 July 2012 to allow more than one day to contact the witnesses after the defense provides a synopsis of the expected testimony sufficient to show its relevance and necessity.

<sup>3</sup> Any disagreements between the parties' questionnaires will be resolved at the 16-20 July 2012 Article 39(a).

<sup>4</sup> The parties will be ready to discuss the case calendar at the 16-20 July 2012 Article 39(a) session.

(B) Article 39(a): 16-20 July 2012

**(13) Defense Notice of Intent to Disclose Classified Information under MRE 505(h) (Charged Documents)**

(A) Filing: 6 July 2012

(B) Response: 11 July 2012

**f. Interim Pretrial Motions (10 August 2012 @ 1300)**

**g. Pretrial Motions (20 July 2012 - 31 August 2012)**

(A) Filing: 3 August 2012

(B) Response: 17 August 2012

(C) Reply: 22 August 2012

(D) Article 39(a): 27-31 August 2012

**(1) Article 13**

(A) Filing: 27 July 2012<sup>5</sup>

**(2) *Motions in Limine***

**(3) *Motions to Suppress (if any)***

**(4) *Due Diligence Ex Parte Filing***

(A) Filing: 25 July 2012

**(5) Notification to the Court of Anticipated Limited Disclosures under MRE 505(g)(2) or Notification to the Court of Privilege under MRE 505(c) for Files under the Possession Custody, or Control of Military Authorities based on the Court's 22 June 2012 Ruling**

(A) Filing: 20 July 2012

**(6) Notification to the Court of Anticipated Limited Disclosures under MRE 505(g)(2) or Notification to the Court of Privilege under MRE 505(c) for FBI Investigative File based on the Court's 22 June 2012 Ruling<sup>6</sup>**

(A) Filing: 25 July 2012

**(7) Government Filing for *In Camera* Proceeding IAW MRE 505(i) with Notice to Defense (if Privilege is Claimed) based on the Court's 22 June 2012 Ruling**

(A) Filing: 25 July 2012

---

<sup>5</sup> The defense agreed to the filing date of one week earlier to give the United States the necessary time to respond.

<sup>6</sup> The United States has already provided the Court with its Motion for Substitutions under MRE 505(g)(2) for FBI Impact Statement.

**(8) Disclosure to Defense or Disclosure to the Court under RCM 701(g)(2) or MRE 505(g)(2) of All Information Subject to the Court's 22 June 2012 Ruling<sup>7</sup>**

(A) Filing: 3 August 2012

**(9) Disclosure of All Remaining Unclassified or Classified (under MRE 505(g)(1)) Brady Material and Disclosure under MRE 701(g)(2) or MRE 505(g)(2) of All Remaining Classified Brady Material<sup>8</sup>**

(A) Filing: 3 August 2012

**(10) Witness Lists for Speedy Trial, including Article 10**

(A) Witness Lists: 10 August 2012

(B) Government Objections (if any): 17 August 2012<sup>9</sup>

(C) Defense Motion to Compel (if any): 22 August 2012

(D) Article 39(a): 27-31 August 2012

**(11) Updated Proposed Case Calendar<sup>10</sup>**

(A) Filing: N/A

(B) Article 39(a): 27-31 August 2012

**h. Interim Pretrial Motions (7 September 2012 - 19 September 2012)**

(A) Filing: 7 September 2012

(B) Response: 14 September 2012

(C) Article 39(a): 19 September 2012

**(1) Defense Notice of Intent to Disclose Classified Information under MRE 505(h) (From Subsequent Disclosures)<sup>11</sup>**

**i. Pretrial Motions (7 September 2012 - 19 October 2012)**

---

<sup>7</sup> This disclosure includes all files that involve investigation, damage assessment, or military measures that are under the possession, custody, or control of military authorities; all FBI files that involve investigation, damage assessment, or mitigation measures; the ODN/ONCIX damage assessment; and evidence the United States will introduce on the merits and during sentencing.

<sup>8</sup> This production includes any material discovered while searching the files, if any, of the President's Intelligence Advisory Board, and all material that is not subject to Motions to Compel Discovery or Production. If the Court rules that any of the proposed summaries under MRE 505(g)(2) are not acceptable, the prosecution will need additional time to obtain approval for a different substitution.

<sup>9</sup> The Court and the parties discussed an objection date of 22 August 2012 in the 25 June 2012 RCM 802 Conference; however, the United States set the date earlier to allow the defense the opportunity to file a motion to compel, if necessary.

<sup>10</sup> The parties will be ready to discuss the case calendar at the 27-31 August 2012 Article 39(a) session.

<sup>11</sup> The defense suggested a filing date of 17 August 2012 and a response date of 22 August 2012; however, the defense suggested timeline does not take into account the time necessary for the Court to review the MRE 505(g)(2) disclosures. The United States, therefore, proposes the disclosure occur in the interim motions hearing.

- (A) Filing: 14 September 2012
- (B) Response: 28 September 2012
- (C) Article 39(a): 15-19 October 2012

**(1) Speedy Trial, including Article 10**

- (A) Filing: 7 September 2012<sup>12</sup>

**(2) Witness List (Defense and Supplemental Government)**

- (A) Filing: 14 September 2012
- (B) Government Objection to Defense Witnesses: 21 September 2012
- (C) Motion to Compel Production: 28 September 2012
- (D) Response: 3 October 2012
- (E) Article 39(a): 15-19 October 2012

**(3) Defense Notice of its Intent to Offer the Defense of Alibi, Innocent Ingestion, or Lack of Mental Responsibility IAW RCM 701(b)(2)**

**(4) Defense Production of Government Reciprocal Discovery Request**

- (A) Date: 14 September 2012

**(5) Government Motion to Compel Discovery (if any)**

- (A) Filing: 28 September 2012
- (B) Response: 3 October 2012
- (C) Article 39(a): 15-19 October 2012

**(6) Defense Notice of Accused's Forum Selection and Notice of Pleas in Writing<sup>13</sup>**

- (A) Filing: 7 September 2012

**j. Interim Pretrial Motions (22 October 2012 - 31 October 2012)**

- (A) Filing: 22 October 2012
- (B) Response: 26 October 2012
- (C) Article 39(a): 31 October 2012

**(1) Updated Proposed Case Calendar (if necessary)**

**(2) Production of Compelled Discovery for Government Motion to Compel Discovery**

- (A) Date: 22 October 2012

**k. Pretrial Motions (2 November 2012 - 30 November 2012)**

---

<sup>12</sup> The defense agreed to the filing date of one week earlier to give the United States the necessary time to respond.

<sup>13</sup> If the accused selects a panel, the United States proposes the panel be notified no less than sixty days prior to trial, in order to coordinate for extended special duty and travel. The 7 September 2012 date was suggested by the defense.

- (A) Filing: 2 November 2012
- (B) Response: 16 November 2012
- (C) Article 39(a): 28-30 November 2012<sup>14</sup>

**(1) Pre-Qualification of Experts**

**(2) Requests for Judicial Notice**

**(3) Supplemental Government Witness List<sup>15</sup> (if necessary)**

**(4) Motions *in Limine* (Supplemental, Including any Classified Information) (if necessary)**

**l. Interim Pretrial Motions (14 November 2012 - 20 December 2012)**

- (A) Filing: 7 December 2012
- (B) Response: 14 December 2012
- (C) Article 39(a): 19-20 December 2012

**(1) Litigation Concerning MRE 505(h) and MRE 505(i)<sup>16</sup>**

- (A) Filing: 14 November 2012
- (B) Response: 27 November 2012<sup>17</sup>
- (C) Article 39(a): 19-20 December 2012

**(2) Updated Proposed Case Calendar (if necessary)**

**m. Pretrial Motions (14 December 2012 - 11 January 2013)<sup>18</sup>**

- (A) Filing: 14 December 2012
- (B) Response: 28 December 2012
- (C) Reply: 2 January 2013
- (D) Article 39(a): 9-11 January 2013

---

<sup>14</sup> The hearing is scheduled one week later than the default schedule due to the Thanksgiving holiday.

<sup>15</sup> The United States will submit a supplemental witness list based solely on any rulings from the government motion to compel discovery ruling and any disclosures by the defense after the 14 September 2012 witness list due date.

<sup>16</sup> This includes *in camera* proceedings for Defense Notice to Disclose Classified Information and/or the Government's Invocation of the Privilege for Merits and Sentencing Information. The United States estimates that any Court order to disclose classified information will likely require coordination with multiple federal organizations and roughly estimates forty-five to sixty days to aggressively coordinate a response across all equity holders.

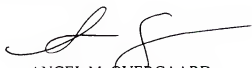
<sup>17</sup> The adjusted date gives the Court additional time to review any discoverable material and was agreed to by the defense. The Government estimates the review will take no more than fifteen duty days to complete.

<sup>18</sup> There have been numerous unplanned motions submitted throughout the pre-trial process. The prosecution, therefore, anticipates that several pretrial motions will be filed under the "Any Additional Motion" timeframe.

- (1) Any Additional Motion that does not have an Identified Deadline
- (2) Grunden Hearing for All Classified Information
- (3) Voir Dire Questions, Flyer, Findings/Sentence Worksheet, All CMCOs
  - (A) Filing for Court Review: 2 January 2013
  - (B) Article 39(a): 9-11 January 2013

n. **Trial by Members (18 January 2013 - 8 February 2013)**

- (A) Voir Dire: 18 January 2013
- (B) Trial: 21 January 2013-8 February 2013



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**Government Response  
to Defense Witness Request:  
Article 13**

**10 July 2012**

The Government has reviewed the Defense witness and evidence requests dated 3 July 2012 (Defense Request). Without the benefit of the Defense's Article 13 Motion, the Government does not know the issues the Defense will raise with respect to Article 13, except for what is apparent in its proffered expected testimony. The Defense Witness Request focuses on the accused's confinement at the Quantico Pretrial Confinement Facility (Quantico Brig). The Defense's proffered testimony for all witnesses does not raise any allegation of improper treatment at the Fort Leavenworth Joint Regional Correctional Facility (JRCF).

Pursuant to Rule for Courts-Martial (RCM) 703(b)(1), the Government makes the following determinations regarding these Defense requested Article 13 witnesses:


1. The Government will produce CAPT William J. Hocter. CAPT Hocter, a psychiatrist, treated the accused and made recommendations regarding the accused and his mental health at Quantico Brig.
2. The Government will produce COL Ricky Malone. COL Malone, a psychiatrist, consulted with CAPT Hocter and also treated the accused and made recommendations regarding the accused and his mental health at Quantico Brig.
3. The Government will produce CAPT Kevin D. Moore. CAPT Moore served previously as a Defense expert consultant in psychiatry. CAPT Moore did not treat the accused.
4. The Government will produce Col. Robert G. Oltman, U.S.M.C. Col. Oltman was the Quantico Security Battalion commander and the supervising commander of the Quantico Brig.
5. The Government will produce LCDR David Moulton. LCDR Moulton served previously as a Defense expert consultant in psychiatry. LCDR Moulton did not treat the accused.
6. The Government denies production of LTC Dawn Hilton. The Defense's proffered testimony of LTC Hilton is not relevant and necessary under RCM 703(b)(1). According to LTC Hilton and the Defense Request, LTC Hilton had neither responsibility for nor interaction with the accused at Quantico Brig. LTC Hilton was the commander for a U.S. Army confinement facility. Quantico Brig was a Marine facility under the command and control of the U.S. Marine Corps. During a telephonic interview with the Government in response to the Defense Request, LTC Hilton stated that she would not question another commander's decisions at a different confinement facility, and that she was the JRCF commander when the accused assaulted another pretrial confinee on 10 December 2011. The Defense Request does not allege that the accused's

confinement at the JRCF violated Article 13. Therefore, any proffered testimony by LTC Hilton would be unrelated and irrelevant to the accused's pretrial confinement at Quantico Brig.

7. The Government denies production of Mr. Juan E. Méndez. The Defense's proffered testimony of Mr. Méndez is not relevant and necessary under RCM 703(b)(1). During a telephonic interview with the Government in response to the Defense Request, Mr. Méndez stated that he never met with the accused, spoke with the accused, nor visited Quantico Brig. Mr. Méndez informed the Government that his only knowledge about the accused and the accused's confinement conditions was through information he received from conversations with Mr. Coombs or he received by public mailings. Additionally, contrary to what the defense proffered, Mr. Méndez offered to meet with the accused at Quantico Brig even though he would be monitored; however, the accused declined to meet with him. Focused on the accused and his confinement conditions, Mr. Méndez ultimately would testify regarding the accused's refusal to meet with him or about information Mr. Méndez learned through Defense Counsel and public notifications. Neither line of testimony is relevant.

Pursuant to Rule for Courts-Martial (RCM) 703(f), the Government makes the following determinations regarding the Defense requested Article 13 evidence:

1. The Government denies production of the Quantico Brig issued suicide prevention smock. Under RCM 703(f)(3), the Defense failed to demonstrate the relevance of the suicide prevention smock. However, assuming the Defense intends to articulate relevance in the future by explaining a need for the Court to see an actual smock in-court, testimony and photographs of the smock will be sufficient for the Court to understand its purpose, limitations, or possible effect. The Government is working to obtain a picture of the smock.
2. The Government denies production of the Quantico Brig issued suicide prevention blanket. Under RCM 703(f)(3), the Defense failed to demonstrate the relevance of the suicide prevention blanket. However, assuming the Defense intends to articulate relevance in the future by explaining a need for the Court to see an actual blanket in-court, testimony and photographs of the blanket will be sufficient for the Court to understand its purpose, limitations, or possible effect. The Government produced a picture of the blanket to the Defense. See Bates# 447860.
3. The Government denies production of the Quantico Brig issued suicide prevention mattress. Under RCM 703(f)(3), the Defense failed to demonstrate the relevance of the suicide prevention bed. However, assuming the Defense intends to articulate relevance in the future by explaining a need for the Court to see an actual mattress in-court, testimony and photographs of the mattress will be sufficient for the Court to understand its purpose, limitations, or possible effect. The Government produced a picture of the mattress to the Defense. See Bates# 447860.

  
ALEXANDER VON ELTEN  
CPT, JA  
Assistant Trial Counsel





ASHDEN FEIN  
MAJ, JA  
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 10 July 2012.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE NOTICE UNDER  
MILITARY RULE OF EVIDENCE  
505(h)(3): CHARGED  
DOCUMENTS ADDENDUM**

DATED: 11 July 2012

1. The Defense previously indicated that Specification 13 of Charge II references 125 diplomatic cables – it actually only references 124. Additionally, only 8 of the 124 cables listed in the charged documents were not part of the OCA's classification review. Bates number 00377526-29, part of the charged documents, refers to the previously believed missing 07BAGHDAD42 cable.

2. Nothing contained in this notice should be construed in any manner as a concession by PFC Manning or his Defense that the listed items are appropriately classified pursuant to Executive Order 13256 or that the disclosure of such information would be detrimental to the national security.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE REPLY TO**

**GOVERNMENT RESPONSE TO**

**RENEWED DEFENSE MOTION**

**TO DISMISS FOR FAILURE TO**

**STATE AN OFFENSE:**

**SPECIFICATIONS 13 AND 14 OF**

**CHARGE II**

DATED: 11 July 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 907(b)(1)(B), requests this Court to dismiss Specifications 13 and 14 of Charge II because the Government has still failed to allege that PFC Manning's alleged conduct exceeded authorized access within the meaning of 18 U.S.C. Section 1030(a)(1).

ARGUMENT

2. The Government Response to the Defense Renewed Motion to Dismiss [hereinafter Government Response] clearly demonstrates that the Government's Wget theory on "exceeds authorized access" is simply a red herring; it is being put forth solely to muddy the waters long enough for the Government to present its evidence to the court-martial members. Perhaps the Government hopes to cling to its assortment of impermissible theories of "exceeds authorized access" just long enough to establish a lesser-included offense for Specifications 13 and 14 of Charge II. Perhaps the Government wishes to prove its case with respect to Specifications 13 and 14 in order to increase the likelihood of a guilty verdict on the other specifications. Whatever its motive, the Government cannot escape the fact that it has no cognizable theory of "exceeds authorized access" that can be applied to PFC Manning's conduct.

3. As a factual matter, it is undeniable that PFC Manning was authorized to access the information covered by Specifications 13 and 14. In its Response, the Government coyly states that it did not stipulate to this fact. The Government, however, also avoids disputing this fact, both in its Response and in all other written and oral representations made to this Court. Moreover, the undisputed evidence and the Government's reliance on its novel theories of "exceeds authorized access" make clear that the Government has no evidence that PFC Manning was not authorized to access the information he allegedly accessed. The Government's attempt to manufacture a factual issue where none exists is not only unsupportable; it borders on bad faith.

4. As to the legal merits of the Government's Wget theory, the Government Response confirms what the Defense anticipated in its Renewed Motion: the Wget theory is simply a new and less

persuasive variant of the worn out (and rejected) expansive interpretation of "exceeds authorized access." The Government fails to identify a single case that supports its theory; this is because there is no case that has permitted a section 1030 claim to proceed based on a pure contract-based "Terms of Use" violation. Moreover, its discussion of the *Nosal* dicta, Professor Orin Kerr's commentary, and the 1996 legislative history is disingenuous. Additionally, the Wget theory would lead to undeniably absurd results. Finally, the Government's suggestion that a court instruction can "balance" an impermissible theory and a permissible one and allow the court-marital members to choose which one to accept is utterly senseless.

5. The Government makes no attempt to address the Defense's argument regarding the Government theory underlying Specification 14 of Charge II. Instead, it advocates, in a single sentence, a "wait and see" approach. The obvious problem with this approach is that the Government cannot be permitted to simply fire a barrage of prejudicial evidence at the members and then, after the smoke has cleared, figure out whether a permissible theory of "exceeds authorized access" fits that evidence. Rather, the time to articulate a cognizable legal theory is now. As the Government has repeatedly demonstrated its inability to articulate such a theory for Specification 14, the dismissal of that specification is long overdue.

6. Finally, both the substance and the tenor of the Government Response shows that the Government's true objective is not to attempt to state a cognizable legal theory for "exceeds authorized access," but rather to delay the day of reckoning for its theory (or theories) until after it has put forth its case to the members. For reasons already stated in the Defense Renewed Motion, any such delay would result in severe prejudice to the accused. The Government offers no response to these concerns. The implication of its silence is clear: the Government either has no response or did not bother to come up with one. Either way, this Court, unlike the Government, cannot cavalierly disregard the concerns of prejudice to an accused.

7. For these reasons, this Court should grant the Defense Renewed Motion and should dismiss Specifications 13 and 14 of Charge II.

**A. It is Undeniable that PFC Manning Was Authorized to Access the Information in Specifications 13 and 14 of Charge II**

8. It is an undeniable fact that PFC Manning was authorized to access the information in Specifications 13 and 14 of Charge II. The Government has never attempted to dispute this fact in any of its representations to this Court. Moreover, the undisputed evidence and the Government's reliance on its novel theories of "exceeds authorized access" make clear that the Government has no evidence that PFC Manning was not authorized to access the information he allegedly accessed. The Government's lack of candor in manufacturing a factual issue where none exists is astonishing.

9. To be clear, this section of the Defense Reply only addresses the issue of whether PFC Manning was authorized to access the information in the first place. It does not deal with the manner in which he allegedly accessed the information or the purposes for which he accessed it. Rather, this section addresses the straightforward question of whether PFC Manning had authority to access the information; in plain terms, was PFC Manning allowed to use his computer to view (i.e. to "obtain" under Section 1030(e)(6)) the information in Specifications 13

and 14 of Charge II? The Government has steadfastly avoided directly answering this question. It has instead jumped immediately to talking about the purposes for which the information was accessed or the precise manner in which the information was downloaded. Since the Government has refused to answer this question, before addressing the merits of the Government's Wget theory, this Reply first demonstrates that PFC Manning was indeed authorized to access the information in question.

10. In its Response, the Government states that "the United States has never stipulated to the fact that the accused was entitled or authorized to access 'each and every piece of information' the accused allegedly accessed on his government computer." Government Response, at 1. However, the Government conveniently neglects to address the Defense assertion that the Government has not disputed that PFC Manning was authorized to access all of the information at issue. See Defense Renewed Motion, at 2. Certainly nothing in the Government's prior Section 1030 filings or representations during oral argument gave any indication that the Government disputed this fact. Even if not stipulating to a fact equates to disputing that fact, which it does not, any attempt to dispute that PFC Manning was authorized to view all of the information in Specifications 13 and 14 of Charge II is belied by the undisputed evidence and by the Government's reliance on its "exceeding authorized access" theories.

11. It is undisputed that the Net Centric Diplomacy Database was on SIPRNET and did not require any password or separate authorization to access. In its 24 May 2012 Response to Defense Motion to Dismiss Specifications 13 and 14 of Charge II for Failure to State an Offense [hereinafter Government Response to First Motion to Dismiss], the Government states that "[t]he Net-Centric Diplomacy Database (NCD), financed by DOD, was developed to provide a full range of diplomatic reporting ('diplomatic cables') to any individual with access to the DOD-controlled SIPRNET. Diplomatic cables were routed to the NCD database or server, and thus made available to individuals with access to the SIPRNET." Government Response to First Motion to Dismiss, at 2. Thus, it is clear that the cables were freely available to anyone with SIPRNET access. It is equally undisputed that CPT Steven Lim directed all of the analysts to look at that database. See Government Response to First Motion to Dismiss, Enclosure 3, at 32 & n.152. Therefore, the undisputed evidence demonstrates beyond hope of contradiction that PFC Manning was authorized to access the information.

12. Moreover, the Government's own theories for "exceeds authorized access" make it obvious that the Government has no evidence that PFC Manning was not authorized to access the information contained in Specifications 13 and 14 of Charge II. Its first theory – the now-rejected explicit purpose-based restriction theory – was articulated in the Government's Response to the first Defense Motion to Dismiss as follows: "The Government's theory is that the accused 'exceeded authorized access' when he violated the Government's explicit purpose-based access restriction on his SIPRNET computer." Government Response to First Motion to Dismiss, at 3. As expected, the Government used its most recent Response to articulate its newest theory: "The Government's theory for Specification 13 of Charge II [is] that the accused 'exceeded authorized access' in violation of 18 U.S.C. § 1030(a)(1) when he obtained the information at issue using an unauthorized program." Government Response, at 3.

13. Both of the Government's theories are telling. If the Government had even a shred of evidence suggesting that PFC Manning was not authorized to access the information in the first place, its theory of "exceeds authorized access" would be uncontroversial: PFC Manning would

have exceeded his authorized access by using his computer to obtain information that he was not entitled to obtain. Of course, the Government has eschewed any reliance on that straightforward theory, and it has focused instead on the purposes for which the information was accessed and the manner in which the information was downloaded. The only conceivable reason why so much ink has already been spilled on the permissibility of these novel theories is that the Government has no evidence that PFC Manning was not authorized to access this information.

14. Indeed, if the Government does have such evidence and nevertheless persists in arguing about the merits of fringe theories of “exceeds authorized access,” then the Government has caused considerable delay in PFC Manning’s trial through either incompetence or bad faith, dilatory tactics. The Government has at no point indicated that it has any evidence showing that PFC Manning was not allowed to view the information covered by Specifications 13 and 14 of Charge II. The undisputed evidence, the Government’s reliance on various “exceeds authorized access” theories, and the Government’s refusal to directly rebut the Defense’s assertions regarding PFC Manning’s authority to access the information all point unwaveringly to the conclusion that PFC Manning was in fact authorized to access the information he accessed.

15. The time for being coy has long past. If candor to the tribunal is anywhere on the Government’s radar, the Government will stop skirting this question and come clean to this Court and the Defense.

#### **B. The Government’s Wget Theory is Not Permissible Under this Court’s Ruling**

16. Returning to the merits of the Wget theory, the Government Response clearly shows that the Wget theory is simply a new (and much less compelling) variant of the already rejected expansive interpretation of “exceeds authorized access.” Unfortunately, the Government still does not seem to understand the *Nosal* holding or the Court’s ruling. If it did, it would never have advanced the argument that it has. The Government says:

Ultimately, if the court thought the issue was black and white- if an individual has access to the information in some capacity, then they cannot exceed authorized access - they would have articulated that draconian concept more clearly.

Government Response, at 4. Unfortunately for the Government, this is not a “draconian concept” – it is the law. And if the Government needs it “articulated . . . more clearly,” the Defense would suggest that it take another look at the Court’s ruling and the cases cited by the Defense. See Appellate Exhibit CXXXIX, at 6 (“Therefore an analysis of the legislative history of the CFAA and the phrase ‘exceeds authorized access’ reveals that the statute is not meant to punish those who use a computer for an improper purpose or in violation of the governing terms of use, but rather the statute is designed to criminalize electronic trespassers and computer hackers.”); *id.* at 9 (Court adopting *Nosal* view of “exceeds authorized access”: “[t]he term] applies to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files”); see also *United States v. Aleynikov*, 737 F. Supp. 2d 173, 191 (S.D.N.Y. 2010) (dismissing CFAA indictment where “[t]he Government concedes that Aleynikov was authorized to access the source code for the Trading System that he allegedly stole[.]”); *United States v. Zhang*, No. CR-05-00812 RMW, 2012 WL 1932843 (N.D. Cal. May 29, 2012) (finding defendant not guilty of Section 1030(a)(4) and (c)(3)(A) violations because

defendant “had ‘authorized access’ to the Marvell Extranet when he downloaded the information from the Marvell Extranet in March 2005 because he had active log-in credentials at that time.”); *Ajuba Int’l, L.L.C. v. Saharia*, No. 11-12936, 2012 WL 1672713, at \*12 (E.D. Mich. May 14, 2012) (holding that “a violation [of the CFAA] for “exceeding authorized access” occurs only where initial access is permitted but the access of *certain information* is not permitted.” (emphasis supplied)); *Ryan, LLC v. Evans*, No. 8:12-cv-289-T-30TBM, 2012 WL 1532492, at \*5 (M.D. Fla. March 20, 2012) (“Under a narrow reading of the provisions of [Section] 1030, a violation for exceeding authorized access occurs where initial access is permitted but the access of *certain information* is not permitted.” (quotations omitted) (emphasis supplied)); *id.* at \*6 (“Given that Evans and Espinosa appear to have had unfettered access to the Ryan computers, *data, information, and emails actually accessed*, with the right to add to, delete from, and upload and download matters therefrom, it is doubtful that their conduct can be brought within the purview of either [Section] 1030(a)(2)(C) or [Section] 1030(a)(4) under the narrow reading of those sections.” (emphasis supplied)); *WEC Carolina Energy Solutions, LLC v. Miller*, No. 0:10-cv-2775-CMC, 2011 WL 379458, at \*4 (D.S.C. Feb. 3, 2011) (“[L]iability under the CFAA, based on an allegation that an employee exceeded authorized access, depends on whether the employee accessed *information* he was not entitled to access. WEC has not alleged that Miller or Kelley accessed information that they were not “entitled to access.” Therefore its allegation falls outside the scope of this portion of the CFAA.” (emphasis supplied)); *Nat’l City Bank, N.A. v. Republic Mortgage Home Loans, LLC*, No. C09-1550RSL, 2010 WL 959925, at \*3 (W.D. Wash. March 12, 2010) (“A CFAA violation occurs only when an employee accesses *information* that was not within the scope of his or her authorization.” (emphasis supplied)); *id.* (“It is undisputed that Westmark was authorized to access, view, and utilize the Excel spreadsheet that forms the heart of plaintiff’s CFAA claim against him. There is no indication that Westmark accessed or obtained any information from National City’s computers after he resigned his position with National City. If, as is the case here, the employee were *entitled to access the materials at issue*, nothing in the CFAA suggests that the authorization can be lost or exceeded through post-access conduct. On the other hand, if an employee’s access is limited to certain documents, files, or drives, an effort on his part to delve into *computer records to which he is not entitled* could result in liability under the CFAA.” (citations omitted) (emphases supplied)); *Lockheed Martin Corp. v. Speed*, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at \*5 (M.D. Fla. Aug. 1, 2006) (“By applying the plain meaning of the statutory terms to the facts of this case, it is clear that the Employees accessed with authorization, did not exceed their authorization, and thus did not violate [Section] 1030(a)(4). The analysis is not a difficult one. Because Lockheed permitted the Employees to access the company computer, they were not without authorization. Further, *because Lockheed permitted the Employees to access the precise information at issue, the Employees did not exceed authorized access*. The Employees fit within the very group that Congress chose not to reach, *i.e.*, those with access authorization. It follows that [Section] 1030(a)(4) cannot reach them. The gist of Lockheed’s complaint is aimed not so much at the Employees’ improper access of the ATARS information, but rather at the Employees’ actions subsequent to their accessing the information. As much as Lockheed might wish it to be so, [Section] 1030(a)(4) does not reach the actions alleged in the Complaint.” (emphasis supplied)).

17. In addition to the reasons identified in the Defense Renewed Motion, there are several other reasons to reject the Wget theory. First and foremost, the Government fails to identify a single case that supports its theory. Additionally, the Government uses the language from *Nosal* and

Professor Orin Kerr in a disingenuous attempt to make a violation of the Acceptable Use Policy (AUP) look like the circumvention of security measures. Moreover, the Government's reading of the 1996 legislative history is incorrect. In addition, the Government's Wget theory would lead to absurd results. Finally, the Government's proposed "balance" of an impermissible theory with a permissible one makes no sense.

i) There is Absolutely No Case Law to Support the Government's "New" Theory

18. The Government has not identified a single case lending any support to its theory that the use of an unauthorized program can make otherwise authorized access to information exceeding authorized access. Not one case. The Government apparently requests that this Court become the first in the nation to adopt this particular variation of the expansive interpretation of "exceeds authorized access."

19. There are only three conceivable theories of how an accused can exceed authorized access to a computer. First, the user can exceed non-purpose based contractual restrictions on access. In other words, this involves the computer user violating any of the various contractual "terms of use" that govern computer access aside from those pertaining to the improper or unauthorized use of information (e.g. restrictions on how old you need to be to access a website, restrictions on permissible software/hardware to be used on the computer, etc.). The expressions "terms of use" are also referred to variously in the case law as "terms of service," "terms of access," "acceptable use policy" and the like. Second, the user can exceed purpose-based restrictions on access – whether explicit or implicit.<sup>1</sup> That is, the computer user can use the information obtained from the computer in a way that is contrary to the purposes for which such information is intended to be used. This second scenario is that contemplated in *Nosal, John and Rodriguez*. Third, the user can bypass technical restrictions on access (e.g. crack a code; guess at a password, etc.), thereby tricking the computer into giving him greater privileges than he otherwise enjoys.

20. These three scenarios can be seen along a spectrum:

THEORY 1	THEORY 2	THEORY 3
Violating	Violating	Bypassing
Contractual	Purpose-Based	Technical
Terms of Use	Restrictions	Restrictions
	On Access	On Access

*LEAST COMPELLING*

*MOST COMPELLING*

<sup>1</sup> Implicit limitations exist where there is no governing "Terms of Use" policy which expressly proscribes using the information for purposes for which the authorization does not extend. Rather, by using agency principles, some courts have held that there is an implicit limitation on a computer user's access, such that he loses authorized access once he uses the computer in a manner contrary to the computer owner's interests. See, e.g. *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7<sup>th</sup> Cir. 2006) ("Citrin's breach of his duty of loyalty terminated his agency relationship (more precisely, terminated any rights he might have claimed as IAC's agent-he could not by unilaterally terminating any duties he owed his principal gain an advantage) and with it his authority to access the laptop, because the only basis of his authority had been that relationship.").



The further one moves to the left of the spectrum, the less compelling the justification for maintaining a Section 1030 violation. All courts recognize that if facts fall within Theory 3, then a Section 1030 violation is cognizable. Courts are split on Theory 2 – i.e. this is the *Nosal*, *Rodriguez*, and *John* line of cases. No court has ever recognized Theory 1, a pure breach of contract, as supporting a 1030 violation. The Government has moved from Theory 2, which the Court (correctly) found to be an impermissible theory, to Theory 1, a theory which is *far less compelling* than Theory 2. If a Court has held that Theory 2 is not viable, it follows as a matter of law that Theory 1 is not viable.

21. The leading case on Theory 1 is *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), which “raise[d] the issue of whether (and/or when will) violations of an Internet website’s terms of service constitute a crime under the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. [Section] 1030.” *Id.* at 451. Otherwise stated, “[the] central question is whether a computer user’s intentional violation of one or more provisions in an Internet website’s terms of services (where those terms condition access to and/or use of the website’s services upon agreement to and compliance with the terms) satisfies the first element of section 1030(a)(2)(C) [exceeds authorized access]. If the answer to that question is “yes,” then seemingly, any and every conscious violation of that website’s terms of service will constitute a CFAA misdemeanor.” *Id.* at 457.

22. In *Drew*, the adult defendant created a false MySpace profile of a teenage boy, posted a picture of a teenage boy to that profile without the boy’s consent, used that profile to befriend a teenage girl, and eventually used that profile to tell that teenage girl that “the world would be a better place without her in it.” *Id.* at 452. The teenage girl took her own life later that day, and the defendant was soon indicted for felony violations of Section 1030(a)(2)(C) and (c)(2)(B)(ii). *Id.* The defendant was alleged to have exceeded her authorized access to MySpace.com because her act of creating the false profile and the posting of a picture of a teenage boy without the boy’s consent violated MySpace’s terms of service. *Id.* That is, the defendant violated non-purpose based contractual terms of service. The jury acquitted the defendant of the felony violations but convicted her on misdemeanor violations of Section 1030(a)(2)(C). *Id.* at 453. The defendant then filed a motion for judgment of acquittal, contending that the violation of the terms of service of an internet provider cannot constitute exceeding authorized access under Section 1030 and, if it did, Section 1030 was unconstitutionally vague. *Id.* at 451.

23. The United States District Court for the Central District of California granted the defendant’s motion, concluding that Section 1030(a)(2)(C), as interpreted by the court and as applied to the defendant’s conduct, was unconstitutionally vague. *Id.* at 464-67. First, the court determined that, as it had interpreted Section 1030, the statute presented serious notice problems: “[T]he language of [S]ection 1030(a)(2)(C) does not explicitly state (nor does it implicitly suggest) that [Section 1030] has ‘criminalized breaches of contract’ in the context of website terms of service. ... Thus, while ‘ordinary people’ might expect to be exposed to civil liabilities for violating a contractual provision, they would not expect criminal penalties.” *Id.* at 464.

24. Second, “if a website’s terms of service controls what is ‘authorized’ and what is ‘exceeding authorization’ – which in turn governs whether an individual’s accessing information or services on the website is criminal or not, [S]ection 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will.” *Id.* The court further noted that “[i]f any violation of any

term of service is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but it would, in turn, render the statute incredibly overbroad and contravene the second prong of the void-for-vagueness doctrine as to setting guidelines to govern law enforcement.” *Id.* at 464-65.

25. Third, the court noted the very common sense proposition that “by utilizing violations of the terms of service as the basis for the [S]ection 1030(a)(2)(C) crime, that approach makes the website owner-in essence-the party who ultimately defines the criminal conduct.” *Id.* at 465. The *Drew* Court concluded that “[t]his will lead to further vagueness problems. The owner’s description of a term of service might itself be so vague as to make the visitor or member reasonably unsure of what the term of service covers.” *Id.* The court further observed that “website owners can establish terms where either the scope or the application of the provision are to be decided by them *ad hoc* and/or pursuant to undelineated standards. For example, the MSTOS [MySpace Terms of Service] provides that what constitutes ‘prohibited content’ on the website is determined ‘in the sole discretion of MySpace.com[.]’” *Id.* The court also expressed concern that the terms of service “may allow the website owner to unilaterally amend and/or add to the terms with minimal notice to users.” *Id.*

26. Thus, the *Drew* court rejected the possibility that contractual terms of service agreements could provide the factual basis to state a Section 1030 claim. And for good reason. Any lay person can see the danger in allowing the computer owner to unilaterally define by contract the scope of a criminal statute which carries with it the possibility of 10 years in prison. To the Defense’s knowledge, no case has ever accepted that non-purpose-based contractual terms of service violations can form the basis for a Section 1030 offense. The Government’s “new” theory falls squarely in Theory 1 – PFC Manning exceeded his authorized access because he used an unauthorized program, proscribed by the terms of use, in order to download information. Accordingly, it should be rejected.

ii) The Government is Trying to Confuse the Court By Pretending that PFC Manning Bypassed Technical Restrictions on Access

27. Perhaps because it recognizes that Theory 1 is dead on arrival, the Government is attempting to confuse this Court by arguing that PFC Manning was an “inside hacker” who “circumvent[ed] procedures,” “hacked the information,” and “bypassed a code-based restriction.” Government Response, at 5. In other words, the Government is attempting to make this look like a Theory 3 scenario. This Court should not be fooled by the Government’s continued deceit.

28. By affixing these labels to the conduct at issue, the Government is trying to bring PFC Manning’s conduct within the *Nosal* holding and Professor Kerr’s construct of technical or code-based restrictions (i.e. Theory 3). Unfortunately, the Government is deliberately distorting language to make it look like there was a “circumvention” of technical restrictions, when in reality – as the Government well knows – there was no such thing. In its desperate attempt to keep a non-cognizable specification on the charge sheet, the Government is trying to manipulate this Court into erroneously believing that to use Wget, one would need to “hack” the computer and bypass security restrictions. Nothing could be further from the truth.

29. The Government states:

The defense is singularly focused on Congress' explanation that § 1030(a)(1) targets those persons who "deliberately break into a computer." See Def. Mot. at 10. However, the Government does not allege the accused hacked "into the computer to obtain information he was not authorized to obtain." Def. Mot. at 10. Instead, he accessed a computer with authorization and exceeded that authorization by circumventing procedures and using an unauthorized program to obtain information—he "hacked" the information. When Congress inartfully summarized § 1030(a)(1) in the 1996 legislative history, they were clearly referring to the "without authorization" prong of § 1030(a)(1). See 18 U.S.C. 1030(a)(1) ("Whoever having knowingly accessed a computer without authorization..."). There is no other logical explanation, because "exceeds authorized access" under 1030(e)(6) necessarily assumes that the individual has accessed a computer with authority in the first place—it criminalizes the "insider" with rights or privileges who misuses a computer. See Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1662 (2003) [hereinafter Kerr, *Cybercrime's Scope*]; *Nosal*, 676 F.3d at 858. Thus, that particular phrase ("deliberately break into a computer"), is misleading if used solely as a basis for defining "exceeds authorized access."

On the other hand, if "deliberately break into a computer" is merely a guiding light in making sense of the purpose of the statute as whole, it contributes to our understanding of "exceeds authorized access." As this Court recognized after considering the legislative history, "the statute is designed to criminalize electronic trespassers and computer hackers." In other words, the statute is designed to criminalize individuals who circumvent or bypass some code-based restriction. See generally Kerr, *Cybercrime's Scope*, at 1600 (using trespassing, hacking, and "bypassing code-based restrictions" somewhat interchangeably). Accordingly, the Government's theory is entirely consistent with the legislative history and this Court's ruling. In order for a person to access or obtain a diplomatic cable on the NCD website, the person has to individually "click" or "save" the diplomatic cable after searching for the cable or navigating to the cable in some manner. As the evidence will show, the accused bypassed the ordinary method of accessing information by adding unauthorized software to his SIPRNET computer and using that software to rapidly harvest or data-mine the information. Wget was not available on the computers used by the accused or authorized as a tool to download the information. See Def. Mot. at 3. Thus, the accused violated a restriction on access to the information – he bypassed a code-based restriction – by using Wget to obtain the cables in batches.

Government Response, at 5.

30. Thus, the Government appears to concede that an accused can only be brought within the purview of the section if the accused bypassed technical or code-based restrictions on access. The Government cites Professor Kerr twice for this proposition. A look at what Professor Kerr

actually said, however, reveals that the Government could not be more off-the-mark in labeling the use of unauthorized software a code-based restriction. Professor Kerr distinguishes between “regulation by code” and “regulation by contract.” Orin S. Kerr, *Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1644-46 (2003). An easy way of understanding this distinction is that “regulation by code” means that the computer owner has inserted some code (i.e. programming language) into the computer which prevents a user from accessing certain information. *See id.* at 1644-45. Regulation by contract means that the computer owner regulates access to the computer by imposing contractual (usually written) limits on the computer user. *See id.* at 1645-46. It is critically important to understand the difference between the two because Professor Kerr maintains (and the case law uniformly bears out) that courts are only concerned with the former for the purposes of Section 1030.

31. Professor Kerr elaborates on the distinction between “Regulation by Code Versus Regulation by Contract” as follows:

Although unauthorized access statutes speak of authorization as if it were a monolithic concept, there are in fact two fairly distinct ways in which access or use of a computer can be unauthorized. Each type corresponds to one of the basic ways that a computer owner can regulate a user’s privileges. A computer owner can regulate a user’s privileges by code or by contract. Similarly, a computer user can engage in computer misuse by circumventing code-based restrictions, or by breaching contract-based restrictions.

When an owner regulates privileges by code, the owner or her agent codes the computers software so that the particular user has a limited set of privileges on the computer. For example, the owner can require every user to have an account with a unique password, and can assign privileges based on the particular account, limiting where the user can go and what she can do on that basis. For a user to exceed privileges imposed by code, the user must somehow “trick” the computer into giving the user greater privileges. I label this approach “regulation by code” because it relies on computer code to create a barrier designed to block the user from exceeding his privileges on the network.

Circumventing regulation by code generally requires a user to engage in one of two types of computer misuse. First, the user may engage in false identification and masquerade as another user who has greater privileges. For example, the user can use another person’s password, and trick the computer to grant the user greater privileges that are supposed to be reserved for the true account holder. If A knows B’s username and password, A can log in to B’s account and see information that B is entitled to see, but A is not.

Alternatively, a user can exploit a weakness in the code within a program to cause the program to malfunction in a way that grants the user greater privileges. Consider a so-called “buffer overflow” attack, a common means of hacking into a computer. A buffer overflow attack overloads the victim computer’s memory

buffer, forcing the computer to malfunction and default to an open position that gives the user "root" or "super user" privileges. These privileges give the user total control over the victim computer: With root privileges, the user can access any account or delete any file. The attack circumvents the code-based restriction that limited the user to her own account. Such misuse violates the intended function test introduced in the Morris case; a user who exploits a weakness in code to trick the victim computer into granting the user extra privileges does so by using the code in a way contrary to its intended function.

The second way an owner may attempt to regulate computer privileges is by contract. The owner can condition use of the computer on a user's agreement to comply with certain rules. If the user has a preexisting relationship with the owner/operator, the conditions may take the form of Terms of Service. If no such relationship exists, the conditions may appear as Terms of Use to the service the computer provides, such as a click-through agreement that might appear prior to use of a website. For example, an adult website may require a user to promise that she is at least eighteen years old before allowing her to access adult materials available through the website. Finally, the restriction may be implicit rather than stated in the written text.

Regulation by contract offers a significantly weaker form of regulation than regulation by code. Regulation by code enforces limits on privileges by actually blocking the user from performing the proscribed act, at least absent circumvention. In contrast, regulation by contract works on the honor system, or perhaps more accurately, the honor system backed by contract law remedies. Consider the adult website that requires users to indicate that they are at least eighteen years old before it allows users to enter. A seventeen-year-old can access the adult website just as easily as an eighteen-year-old can. The only difference is that the seventeen-year-old must misrepresent her age to access the site. To use a physical-world analogy, the difference between regulation by code and regulation by contract resembles the difference between keeping a stranger out by closing and locking the door and keeping a stranger out by putting up a sign in front of an open front door saying "strangers may not enter."

*Id.* at 1644-46 (footnotes omitted).

32. As is clear from the above passage, the notion of inside hackers who circumvent technical restrictions refers to a user who "somehow 'trick[s]' the computer into giving the user greater privileges." *Id.* at 1644. The reason it is called "regulation by code" is because it relies on *computer code to create a barrier* designed to block the user from exceeding his privileges on the network. *Id.* at 1644-45. That is, "[r]egulation by code enforces limits on privileges by actually blocking the user from performing the proscribed act." *Id.* at 1646. Kerr identifies only two ways that a user can circumvent regulation by code.

33. First,

the user may engage in false identification and masquerade as another user who has greater privileges. For example, the user can use another person's password, and trick the computer to grant the user greater privileges that are supposed to be reserved for the true account holder. If A knows B's username and password, A can log in to B's account and see information that B is entitled to see, but A is not.

*Id.* at 1644. There is no evidence the PFC Manning used another user's privileges to gain access to the computer or information in question.

34. Second, "a user can exploit a weakness in the code within a program to cause the program to malfunction in a way that grants the user greater privileges." *Id.* at 1645. Again, there is no evidence that PFC Manning exploited a technical weakness in the code to cause a program to malfunction and thereby obtain greater privileges.

35. These are the exact two code-based restrictions that are highlighted in *Nosal* itself and that are cited by the Government in its Response:

Suppose an employer keeps certain information in a separate database that can be viewed on a computer screen, but not copied or downloaded. If an employee *circumvents the security measures*, copies the information to a thumb drive and walks out of the building with it in his pocket, he would then have obtained access to information in the computer that he is not "entitled so to obtain." Or, let's say an employee is given full access to the information, provided he logs in with his username and password. In an effort to cover his tracks, he *uses another employee's login to copy information from the database*. Once again, this would be an employee who is authorized to access the information but does so in a manner he was not authorized "so to obtain."

*United States v. Nosal*, 676 F.3d 854, 858 (9th Cir. 2012) (en banc) (emphases supplied); see Government Response, at 3-4.

36. The first example in the *Nosal* quote corresponds to Professor Kerr's second code-based limitation, while the second example in the *Nosal* quote corresponds to Professor Kerr's first code-based limitation. The bottom line – whether one looks to *Nosal* or Professor Kerr (who the Defense submits provided the basis for the *Nosal* holding) – is that in order to fall within Section 1030, one must bypass the computer code that creates a barrier between the user and the information in question. If one does not "break" the computer code technical barrier, then one does not exceed authorized access.

37. Apparently, the Government simply does not understand (or is deliberately "misunderstanding") what a code-based restriction is. The Government states, "Thus, the accused violated a restriction on access to the information - he bypassed a code-based restriction - by using Wget to obtain the cables in batches." Government Response, at 5. The passage shows that the Government has no clue what it means to bypass a code-based restriction. If it did, the Government would have specified the "code" (i.e. the computer programming barrier) that PFC Manning allegedly circumvented. The reason it did not, of course, is because PFC

Manning did not need to circumvent a code-based restriction – no such restriction existed.

38. The focus on the circumvention of security measures as the touchstone of “exceeds authorized access” is in perfect harmony with the holdings of *Nosal* and other courts, as well as this Court’s ruling and the 1996 legislative history. Both the *Nosal* Court and this Court have held that the term “exceeds authorized access” applies to “inside hackers.” See *Nosal*, 676 F.3d at 858 (“‘exceeds authorized access’ would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized *information or files*).” (second emphasis supplied)); Appellate Exhibit CXXXIX, at 7 (“*Nosal III* defines ‘exceeds authorized access’ to apply to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files.” (emphasis in original)); 8 June 2012 Article 39(a) audio (“‘exceeds authorized access’ would apply to ‘inside hackers’, individuals whose initial access to a computer is authorized but who access *unauthorized information or files*.” (emphasis supplied)); see also *Aleynikov*, 737 F. Supp. 2d at 191-92 (“a person who ‘exceeds authorized access’ has permission to access the computer, but not the *particular information* on the computer that is at issue.” (emphasis supplied)). Like these cited cases, the 1996 legislative history explains the concept of “exceeds authorized access” with reference to a hacker (i.e. one who breaks into a computer to obtain information). See S. Rep. No. 104-357, at 6 (1996) (“Section 1030(a)(1) would target those persons who *deliberately break into a computer* to obtain properly classified Government secrets then try to peddle those secrets to others, including foreign governments.” (emphasis supplied)).

39. The Government maintains that its theory is consistent with the 1996 legislative history. It is not. The Government states:

Additionally, the Government’s theory for Specification 13 is consistent with the language of the legislative history because it is anchored to the accused’s egregious use of unauthorized software on a government-owned SIPRNET computer. As Congress noted in discussing the difference between § 793(e) and 1030(a)(1), “it is the use of the computer that is being proscribed, not the unauthorized possession of, access to, or control over the classified information itself.” Section 793(e) is focused on the unauthorized possession and transmission of the information, while § 1030 is focused on the misuse of a computer. Wget, despite the wildly erratic defense argument to the contrary, is focused on the use of the computer, not the use of the information.

Government Response, at 5-6. When Congress notes that “it is the use of the computer that is proscribed” this must be viewed in reference to the concept of electronic trespassing referred to above (“deliberately break into a computer”).<sup>2</sup> When one breaks into a computer – whether one is an outside hacker or an inside hacker – one has committed a *crime against the computer*.<sup>3</sup> The use of Wget to download information is not a crime against the computer. It is not electronic trespassing. It is not hacking. It is not circumventing technical or code-based restrictions. Accordingly, nothing about the Government’s “new” theory is consistent with the legislative

<sup>2</sup> The Government would prefer if we simply ignored the literal meaning of this language and used it as “a guiding light.” It is not the guiding light; it is the test ultimately adopted in *Nosal* and by this Court.

<sup>3</sup> Just as if one has committed a trespass, one has committed a crime against the property.

history.

40. In this case, it is clear – despite the Government’s highly disingenuous submission to the contrary – that PFC Manning did not circumvent code-based restrictions to access the information in question. There was no technical code “blocking [PFC Manning] from performing the proscribed act.” Kerr, *supra*, at 1646. The Government, however, is hoping that by using Kerr-like language to distort the actual facts, this Court will fall into the trap of believing that the Government has evidence that PFC Manning bypassed technical restrictions. Of course, the Government has no such evidence.

41. Contrary to its assertions, what the Government is actually alleging is a pure contract-based theory (what the Defense calls Theory 1). According to Professor Kerr, the “owner can condition use of the computer on a user’s agreement to comply with certain rules. If the user has a preexisting relationship with the owner/operator, the conditions may take the form of Terms of Service.” *Id.* at 1645 (footnote omitted). Professor Kerr describes the difference between code-based and contract-based regulation as follows: “Regulation by code enforces limits on privileges by actually blocking the user from performing the proscribed act, at least absent circumvention. In contrast, regulation by contract works on the honor system, or perhaps more accurately, the honor system backed by contract law remedies.” *Id.* at 1646. Here, PFC Manning was not permitted to use Wget to download any information on the computer because it was an unauthorized program under the AUP (for which PFC Manning is *already* separately charged under Article 92). This is a textbook example of a contract-based restriction. The only reason PFC Manning could not use Wget was because it was not on a “list” of approved software – not because the Army included code in the computer that prevented PFC Manning from using the software, which he then circumvented.

42. Professor Kerr’s real world analogy for this distinction is instructive: “the difference between regulation by code and regulation by contract resembles the difference between keeping a stranger out by closing and locking the door and keeping a stranger out by putting up a sign in front of an open front door saying ‘strangers may not enter.’” *Id.* at 1646. In this case, the analogy can be taken one step further. Here, we have the equivalent of a sign that reads “strangers may enter, but they may not enter in a particular manner.”

43. The Government has not been forthright with the Court in the past. When asked whether the Government had evidence *aside from the AUP* that PFC Manning had bypassed restrictions on access, the Government said “yes.” Audio, Oral Argument; Appellate Exhibit CXXXIX, at 9. It did not. All it has is a different section of *the very same AUP*. This is particularly disheartening because the Court conditioned its ruling upon the Government’s misrepresentation that it had evidence “aside from the AUP.” Appellate Exhibit CXXXIX, at 9. In short, the Defense submits that the Government took great liberties with the truth – which, in turn, caused the Court to not dismiss charges which should have been dismissed. In this respect, the Defense submits that the Government had once again demonstrated a lack of candor with the Court.

44. As if that weren’t enough, the Government is not being forthright with the Court once again. Rather than properly conceding that PFC Manning did not bypass technical restrictions (i.e. there was no code-based computer security gate that PFC Manning had to circumvent to use Wget), the Government is purposely warping language in order to keep a fatally defective specification



alive. The Government, of course, has distorted language in the past.<sup>4</sup> It is doing so again. The Government is trying desperately to use all the right words (“circumvent[ed] procedures,” “hacked the information,” and “bypassed a code-based restriction”) so that it can pull the wool over this Court’s eyes. It cannot be permitted to do this.

45. Under no stretch of the imagination can the Government’s Wget theory be squared with this Court’s adoption of the narrow interpretation of “exceeds authorized access.” The Government’s new theory hinges on the use of an unauthorized program to perform what would otherwise be authorized tasks. The obligation to refrain from using unauthorized programs is created by the AUP. See Government Response to First Motion to Dismiss, Enclosure 6, at 62 (“d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software.”). The Government, spurned in its first attempt to make a violation of one provision of the AUP “exceeding authorized access,” has now simply picked a different provision of the same AUP for its “new” theory. In short, the Government has proceeded under Theory 1, even though it tries to dress it up as Theory 3. Since no court has ever allowed Theory 1 to proceed, and because Theory 1 provides an even less compelling rationale than Theory 2 (which has already been rejected by the Court), the specifications must be dismissed.

iii) The Government’s “New” Theory Leads to Even More Absurd Results than Its Previous “Definitive” Theory

46. The Government’s “new” theory leads to even more absurd results than its prior “definitive” theory. To illustrate this point, imagine PFC Manning used Excel 2009 to export (i.e. download) the information in Specifications 13 and 14 of Charge II. Imagine further that Excel 2009 was an authorized program and that the 2009 version of Excel was the only version of Excel authorized to be used on his government computer. Even under the Government’s new theory, his conduct would not constitute “exceeds authorized access,” since the Government cannot dispute that PFC Manning was allowed to view (i.e. authorized to obtain) this information. See Part A, *supra*. However, if PFC Manning had updated the version of Excel on his computer to Excel 2010 – an unauthorized version of Excel – and had downloaded the exact same information in the exact same way, he would have “exceeded authorized access” under the Government’s new theory. Thus, the Government’s theory would make ten years imprisonment based on the exact same conduct hinge solely on which version of Excel PFC Manning used. See 18 U.S.C. § 1030(c)(1)(A) (providing for a maximum of ten years imprisonment for a violation of Section 1030(a)(1)); see also Defense Renewed Motion, at 6 (providing a similar example using Internet Explorer and Firefox). Further, if PFC Manning used Excel 2010 to download all the cables for use in his job (i.e. he did not disclose the cables to unauthorized persons), he could still be subject to criminal prosecution under Section 1030. See 18 U.S.C. § 1030(a)(2)(C) (requiring only that the defendant “exceed authorized access” and obtain information from a protected computer).

47. Moreover, the Government’s new theory is not limited to mere violations of this particular provision of the AUP. Conceivably, any violation of the AUP would render a user’s access to

---

<sup>4</sup> Recall the Government indicating: a) that it was “unaware” of forensic results; b) that ONCIX did not have an interim or a final damage assessment; c) that there was a distinction between “investigation” and “damage assessment”; d) that the DOS has not “completed” a damage assessment, etc.

information unauthorized in the Government's view. See *Drew*, 259 F.R.D. at 464-65 ("[I]f a website's terms of service controls what is 'authorized' and what is 'exceeding authorization' – which in turn governs whether an individual's accessing information or services on the website is criminal or not, section 1030(a)(2)(C) would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will. If *any* violation of *any* term of service is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but it would, in turn, render the statute incredibly overbroad and contravene the second prong of the void-for-vagueness doctrine as to setting guidelines to govern law enforcement.").

48. The Government argues that "the accused bypassed the *ordinary method* of accessing information by adding unauthorized software to his SIPRNET computer and using that software to rapidly harvest or data-mine the information." Government Response, at 5 (emphasis supplied). It fails to recognize, however, that *any* violation of the AUP would bypass the "ordinary method," *id.*, of accessing information on a government computer, since the AUP itself sets forth the ordinary method of accessing information.

49. The very next line of the AUP after the requirement that computer users not install or use unauthorized software requires the use of virus-checking procedures before a user accesses information from certain sources. See Government Response to First Motion to Dismiss, Enclosure 6, at 62 ("e. I will use virus-checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk."). Would failure to use virus-checking procedures before accessing information from a system constitute exceeding authorized access? Not under any sensible interpretation of that term. But under the Government's theory, such a failure would constitute exceeding authorized access because it would bypass the "ordinary method of accessing information" as defined in the AUP. Government Response, at 5. And such a failure alone would, under the Government's view, subject a user to conviction and up to a year imprisonment under Section 1030(a)(2)(C). See 18 U.S.C. § 1030(a)(2)(C) (requiring only that the defendant "exceed authorized access" and obtain information from a protected computer);<sup>5</sup> *id.* § 1030(c)(2)(A) (providing punishment for a violation of Section 1030(a)(2)); *Nosal*, 676 F.3d 859 (explaining that interpretation of "exceeds authorized access" chosen by the Court must apply to all provisions of Section 1030 using that phrase).

50. Similarly, the provision of the AUP that precedes the requirement that computer users not install or use unauthorized software provides that computer users must have secure passwords. See Government Response to Defense Motion to Dismiss, Enclosure 6, at 62 ("c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase and lowercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.")). Would failure to use a sufficiently secure password (e.g. BradleyManning1234) mean that a user

---

<sup>5</sup> To "obtain information" includes merely reading information. See *Drew*, 259 F.R.D. at 457 ("As also stated in Senate Report No. 104-357, at 7 (1996), *reprinted* at 1996 WL 492169 (henceforth "S.Rep. No. 104-357"), "... the term 'obtaining information' includes merely reading it.")

would exceed authorized access when he then logged onto the computer? Again, under the Government's theory, the answer would be yes. There is no logical basis for distinguishing between the various contractual restrictions on computer access/use. Any and all violations of restrictions outlined in the AUP would be punishable criminally.

51. Moreover, there is no requirement that any of the restrictions be reasonable. If the Army wanted to, it could write into the AUP that "Every soldier, prior to accessing a U.S. Army computer, must sing the national anthem." See Government Response to First Motion to Dismiss, Enclosure 6, AR25-2, B-2 ("Army organizations may tailor the information in the sample AUP to meet their specific needs, as appropriate."). A failure to sing the national anthem prior to accessing the computer would then subject the soldier to jail time.

52. One need not be Oliver Wendell Holmes to see that the Government's theory is flat out preposterous. It simply replaces one variation of the expansive interpretation of the phrase "exceeds authorized access" (based on a violation of one provision of the AUP) with another variation of that same expansive interpretation (based on a different provision of the same AUP). However, the Government's theory now is even more ludicrous because it does not depend on a purpose-based limitation on access. A violation of any contractual term of access/use/service would be a violation of Section 1030.

53. The Government cannot sensibly explain how this new theory can be reconciled with this Court's adoption of the narrow interpretation of the phrase "exceeds authorized access." Indeed, it is beyond comprehension how the Government can still pursue in good faith any theory of "exceeds authorized access" based on a violation of the AUP after this Court definitely held that "the term 'exceeds authorized access' is limited to violations of restrictions on *access* to information, and not restrictions on its 'use'." Appellate Exhibit CXXXIX, at 9 (emphasis in original); see also *id.* at 6 ("Therefore an analysis of the legislative history of the CFAA and the phrase 'exceeds authorized access' reveals that the statute is not meant to punish those who use a computer for an improper purpose *or in violation of the governing terms of use*, but rather the statute is designed to criminalize electronic trespassers and computer hackers.").

iv) The Court is Not Permitted to "Balance" Legal Theories: Either an Offense is Cognizable or it is Not

54. Finally, the Government's argument that its proposed instruction balances the competing theories of the Government and the Defense makes no sense. Perhaps in denial, the Government refuses to acknowledge that its expansive purpose-based restriction theory was definitely rejected by this Court. As explained in this Reply and in the Renewed Defense Motion, the Government's Wget theory is even more impermissible than its purpose-based restriction theory. An impermissible theory cannot be "balanced" with a permissible theory in a jury instruction, so that the members decide which legal theory to accept. The members do not decide the proper interpretation of a statute.

55. For these reasons and the reasons articulated in the Defense Renewed Motion, this Court should reject the Government's plea for a revival of the expansive interpretation and should accordingly dismiss Specifications 13 and 14 of Charge II.

**C. The Government Has Offered No Permissible Theory for Specification 14 of Charge II**

56. The Government does not even try to address the Defense's argument regarding the Government theory underlying Specification 14 of Charge II. Instead, it endorses an impermissible "wait and see" approach. However, the time to articulate a cognizable legal theory is now, not at the close of evidence. The reason it has not done so is obvious: it does not have a cognizable legal theory. As such, Specification 14 must be dismissed.

57. The Defense Renewed Motion clearly explained that the forensic evidence unequivocally established that PFC Manning did not use Wget to obtain the information in Specification 14 of Charge II. *See* Defense Renewed Motion, at 10-11. Since the only theory articulated by the Government that could therefore be applied to Specification 14 was its now-rejected explicit purpose-based theory, the Defense Renewed Motion argued that Specification 14 should be dismissed.

58. The Government responded to the Defense's contentions in the last sentence of its Response. It stated that "[t]he United States maintains that its theory of criminal liability for Specification 14 is dependent upon instructions by the Court." Government Response, at 7. This is no response at all.

59. For one thing, the Government has things backwards. While it may prefer to just present its Section 1030 case without putting much thought into its theory of "exceeds authorized access" for Specification 14 of Charge II, the prejudice concerns to PFC Manning identified in the Defense Renewed Motion preclude the Government from doing so. *See* Defense Renewed Motion, at 11-13. The Government's theory cannot be dependent upon this Court's instructions; rather, this Court's instructions must be dependent on the Government's theory, provided it can articulate a cognizable one.

60. For too long, the Government has refused to fully articulate its theory or theories for "exceeds authorized access." When asked as part of the bill of particulars motion what its legal theory was for section 1030, the Government refused to provide an answer. The Government finally did articulate its "definitive" theory in its first Response. Once it lost that motion, the Government's "definitive" theory gave way to cryptic indications that it had other evidence and theories. And after all this, the Government continues to be cagey with its theory for Specification 14. The time to speak is now. Either it has a cognizable legal theory for Specification 14 of Charge II or it does not. If it does not, it should just say so and stop the delay that results from its meritless arguments to the contrary.

**D. This Court Should Put an End to the Government's Delay Tactics**

61. Both the substance and the tenor of the Government Response shows that the Government's true objective is not to attempt to state a cognizable legal theory for "exceeds authorized access," but rather to delay the day of reckoning for its theory (or theories) until after it has put forth its case to the members. For reasons already stated in the Defense Renewed Motion, any such delay would result in severe prejudice to the accused. The Government offers absolutely no response to these concerns – perhaps because it knows that its tactics are indeed deliberately designed to

cause prejudice to the accused. This Court, unlike the Government, does not have the luxury of so blithely disregarding the concerns of prejudice to an accused.

62. The Defense Renewed Motion put forth several prejudice concerns that would arise if the Government is given a free pass on articulating a cognizable legal theory until after the evidence has been presented. *See* Defense Renewed Motion, at 11-13. Those concerns need not be reproduced here.

63. In its Response, the Government offers no rebuttal to these prejudice concerns. Instead, the Government, without even acknowledging these concerns, requests in the alternative that this Court “defer ruling on this motion until the presentation of evidence.” Government Response, at 7. The Government’s decision to avoid responding to the prejudice concerns is telling; either the Government deemed these concerns too insubstantial to even warrant a response or too insurmountable to even attempt one. Either way, the Government, through its silence, seeks to sweep these prejudice concerns under the rug, hoping that this Court will overlook them just as the Government has done.

64. Of course, this Court cannot treat these prejudice concerns as dismissively as the Government has treated them. There can be no deferment on the issue of whether the Government has a cognizable theory of “exceeds authorized access.” No matter how much the Government may wish it were otherwise, a cognizable legal theory is a prerequisite to the presentation of even a single piece of evidence on the Section 1030 specifications. The Government has been challenged to come forward with a permissible theory for “exceeds authorized access.” It has yet to do so. It cannot now request that the Court wait to see what the evidence bears out. Given the history of the Government’s conduct in both the Section 1030 motions and argument and other aspects of this case, the Government is not entitled to the benefit of the doubt that such a “wait and see” approach would give it. Even if it were so entitled, deferment of this issue until after presentation of the Government’s evidence would result in irreversible prejudice to PFC Manning. *See* Renewed Defense Motion, at 11-13. This Court should not permit the Government to delay this matter any longer.

**E. The Government’s Response to this Motion is the Latest in a Long List of Instances Where the Government has not been Candid with the Court**

65. As may be apparent from recent motions practice, the Defense is increasingly troubled by the Government’s lack of candor. We have seen the lack of candor play out particularly in recent discovery dispute. However, we have also seen this elsewhere (e.g. in the Article 104 motion and the motion for a bill of particulars). It is time for the Government to begin taking its ethical responsibilities as officers of the Court more seriously.

66. Here, the facts are not in dispute – however, the Government is making it look like they are. The uncontroverted facts are these:

- Anyone with SIPRNET access had access to the diplomatic cables on the Net-Centric Diplomacy database;
- There were no password restrictions on the Net-Centric Diplomacy database;
- Any and all diplomatic cables could be downloaded by anyone with SIPRNET access;

- There were no restrictions (either technical or contract-based) on the quantity of cables that could be downloaded from the Net-Centric Diplomacy database;
- There were no technical restrictions that electronically blocked users from employing Wget, or any type of authorized or unauthorized software, from downloading cables from the Net-Centric Diplomacy database.

67. Thus, there are three basic questions that the Government continually dances around in an effort to fabricate a factual issue:

*Question One: Did PFC Manning have permission to view the diplomatic cables on the SIPRNET?* The answer here is “yes.” The Government, in an effort to confuse the Court, states that it did not stipulate to this fact. It doesn’t need to. There is no factual question that all persons who had SIPRNET access had access to the diplomatic cables.

*Question Two: Did PFC Manning have permission to download the diplomatic cables?* Again, the answer here is “yes.” As the Government states, PFC Manning was permitted to download the diplomatic cables – though under the AUP, he should have used an authorized program.

*Question Three: Did PFC Manning have to bypass a technical code-based restriction (i.e. some sort of electronic gate) to download the cables using Wget?* The answer here is “no.” There was no code or programming in the computer that physically prevented a user from employing an unauthorized program (Wget or otherwise) to download the information. The source of the restriction on using Wget is found solely in the contractual terms of use.<sup>6</sup>

68. If the Government were honest with itself – and more importantly with the Court – it would admit the truth of the aforementioned. Its continued obfuscation, in keeping with its motions practice in the rest of the case, far exceeds the outer boundaries of zealous advocacy.

69. Not only has the Government continued to play hide the ball with clearly undisputed facts, it has also played hide the ball with the Court as to the evidence it has in its possession. This Court’s denial of the Defense Motion to Dismiss Specifications 13 and 14 of Charge II was based solely on the Government’s representations that it had evidence aside from the AUP. In denying the Defense Motion, this Court explained:

Whether the Court should dismiss the Specifications before presentation of evidence depends on whether the issue is capable of resolution without trial on the issue of guilt. In this case, the Government stated in oral argument that it would *present evidence in addition to the AUP*. The Court does not find that the issue is capable of resolution prior to presentation of the evidence.

---

<sup>6</sup> One might add a fourth question: *Is there evidence that PFC Manning used Wget with respect to the cable in Specification 14?* The answer is clearly “no.” However, the Defense submits that the answer to that question is actually irrelevant because even if PFC Manning had used Wget with respect to the information in Specification 14, this would still not state a cognizable section 1030 offense.

Appellate Exhibit, CXXXIX, at 9 (emphasis supplied). Well, what is the Government's evidence "in addition" to the AUP? There is no such evidence. At the very least, the Government, instead of waiting idly by for a renewed motion to dismiss from the Defense, should have alerted the Court to the fact that the "new evidence" is simply a different section of the *same* AUP.

#### CONCLUSION

70. For the reasons articulated above and in the Renewed Defense Motion, the Defense requests this Court to dismiss Specifications 13 and 14 of Charge II because the Government has still failed to allege that PFC Manning's alleged conduct exceeded authorized access.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

SF 86

Questionnaire For National Security Positions

SF 328

Certificate Pertaining to Foreign Interests

## **Appendix B**

### **Sample Acceptable Use Policy**

#### **B-1. Purpose**

This appendix provides a sample AUP that may be used by organizations to obtain explicit acknowledgements from individuals on their responsibilities and limitations in using ISs.

#### **B-2. Explanation of conventions in sample acceptable use policy**

Figure B-1, below, illustrates a representative AUP. In this figure, text appearing in italicized font should be replaced with the appropriate information pertinent to the specific AUP being executed. Army organizations may tailor the information in the sample AUP to meet their specific needs, as appropriate.



---

### Acceptable Use Policy

**1 Understanding:** understand that I have the primary responsibility to safeguard the information contained in *classified network name (CNN)* and/or *unclassified network name (UNN)* from unauthorized or inadvertent modification, disclosure, destruction, denial of service, and use

**2 Access:** Access to *this/these network(s)* is for official use and authorized purposes and as set forth in DoD 5500.7-R, "Joint Ethics Regulation" or as further limited by this policy

**3 Revocability:** Access to Army resources is a revocable privilege and is subject to content monitoring and security testing

**4 Classified information processing:** CNN is the primary classified *S* for *(insert your organization)*. CNN is a US-only system and approved in process *(insert classification)* collateral information as well as *(insert additional caveats or handling instructions)*. CNN is not authorized to process *(insert classification or additional caveats or special handling instructions)*

a. CNN provides communication to external DoD (or specify other appropriate US Government) organizations using the SIPRNET. Primarily this is done via electronic mail and internet networking protocols such as web, ftp, telnet *(insert others as appropriate)*

b. The CNN is authorized for SECRET or lower-level processing in accordance with accreditation package number, identification, etc

c. The classification boundary between CNN and UNN requires vigilance and attention by all users. CNN is also a US-only system and not accredited for transmission of NATO material

d. The ultimate responsibility for ensuring the protection of information lies with the user. The release of TOP SECRET information through the CNN is a security violation and will be investigated and handled as a security violation or as a criminal offense

**5 Unclassified Information Processing:** UNN is the primary unclassified automated administration tool for the *(insert your organization)*. UNN is a US-only system.

a. UNN provides unclassified communication to external DoD and other United States Government organizations. Primarily this is done via electronic mail and internet networking protocols such as web, ftp, telnet *(insert others as appropriate)*

b. UNN is approved to process UNCLASSIFIED, SENSITIVE information in accordance with *(insert initial regulation dealing with automated information system security management program)*

c. The UNN and the Internet, as viewed by the *(insert your organization)*, are synonymous. E-mail and attachments are vulnerable to interception as they traverse the SIPRNET and Internet

### THEORY 2: Purpose-Based Restriction on Access

---

Figure B. 1. Acceptable use policy

**6. Minimum security rules and requirements.** As a *CNN* and/or *UNN* system user, the following minimum security rules and requirements apply

THEORY 1:  
Contractual  
Terms of Use

- a. Personnel are not permitted access to *CNN* and *UNN* unless in complete compliance with the (insert your organization) personnel security requirement for operating in a TOP SECRET system-high environment
- b. I have completed the user security awareness training module. I will participate in all training programs as required (inclusive of threat identification, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before receiving system access
- c. I will generate, store, and protect passwords or pass-phrases. Passwords will consist of at least 10 characters with 2 each of uppercase letters, numbers, and special characters. I am the only authorized user of this account. (I will not use user ID, common names, birthdays, phone numbers, military acronyms, call signs, or dictionary words as passwords or pass-phrases.)
- d. I will use only authorized hardware and software. I will not install or use any personally owned hardware, software, shareware, or public domain software
- e. I will use virus checking procedures before uploading or accessing information from any system, diskette, attachment, or compact disk
- f. I will not attempt to access or process data exceeding the authorized IS classification level.
- g. I will not alter, change, configure, or use operating systems or programs, except as specifically authorized
- h. I will not introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code
- i. I will safeguard and mark with the appropriate classification level all information created, copied, stored, or disseminated from the IS and will not disseminate it to anyone without a specific need to know
- j. I will not utilize Army- or DoD-provided ISs for commercial financial gain or illegal activities
- k. Maintenance will be performed by the System Administrator (SA) only
- l. I will use screen locks and log off the workstation when departing the area
- m. I will immediately report any suspicious output, files, shortcuts, or system problems to the (insert your organization) SA and/or IASO and cease all activities on the system
- n. I will address any questions regarding policy, responsibilities, and duties to (insert your organization) SA and/or IASO

Figure B-1 Acceptable use policy—Continued

o. I understand that each IS is the property of the Army and is provided to me for official and authorized uses. I further understand that each IS is subject to monitoring for security purposes and to ensure that use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the IS and may have only a limited expectation of privacy in personal data on the IS. I realize that I should not store data on the IS that I do not want others to see.

p. I understand that monitoring of (CNN) (UN\*) will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution. I understand that the following activities define unacceptable uses of an Army IS:

*(insert specific criteria)*

- to show what is not acceptable use
- to show what is acceptable during duty/non-duty hours
- to show what is deemed proprietary or not releasable (key word or data identification)
- to show what is deemed unethical (e.g., spam, profanity, sexual content, gaming)
- to show unauthorized sites (e.g., pornography, streaming video, E-Bay)
- to show unauthorized services (e.g., peer-to-peer, distributed computing)
- to define proper email use and restrictions (e.g., mass mailing, hoaxes, auto-forwarding)
- to explain expected results of policy violations (1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup>, etc)

*(Note: Activity in any criteria can lead to criminal offenses.)*

q. The authority for soliciting a social security number (SSN) is EO 939. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of information is voluntary, however, failure to disclose information could result in denial of access to *(insert your organization)* information systems.

**7. Acknowledgement.** I have read the above requirements regarding use of *(insert your organization)* access systems. I understand my responsibilities regarding these systems and the information contained in them.

*insert name here*  
Directorate/Division/Branch

*insert date here*  
Date

*insert name here*  
Last Name, First MI

*insert Rank/Grade and SSN here*  
Rank/Grade/ SSN

*insert name here*  
Signature

*insert phone number here*  
Phone Number

Figure B. 1. Acceptable use policy --Continued

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE REPLY TO  
GOVERNMENT RESPONSE TO  
DEFENSE MOTION FOR  
SPECIFIC INSTRUCTIONS: THE  
SPECIFICATION OF CHARGE I**

DATED: 11 July 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 920(c), requests this Court to give the instructions requested in the Defense Motion for Specific Instructions: The Specification of Charge I [hereinafter Defense Motion] and the Defense Requested Instruction: Article 104 [hereinafter Defense Requested Instruction].

ARGUMENT

2. The Government is incorrect that a "knowingly and intentionally" requirement for the actual knowledge element of Article 104, 10 U.S.C. § 904, Uniform Code of Military Justice (UCMJ), would transform Article 104 into a specific intent offense. Indeed, it is the Government's proposed definition of "knowingly" that would transform Article 104 into something that it is not – namely, an Article that punishes negligent acts. Finally, the Government's attempt to distinguish the mens rea standard of Offense 26 of the Military Commissions Act from the mens rea required for Article 104 is meritless.

3. Thus, for these reasons, this Court should give the Article 104 instructions requested by the Defense.

**A. A "Knowingly and Intentionally" Requirement Does not Render Article 104 a Specific Intent Offense**

4. The Defense Motion carefully explained that the "intentionally" component of its proposed "knowingly and intentionally" requirement was not to be understood as converting Article 104 into a specific intent offense. Nevertheless, the Government, either misunderstanding the Defense's arguments to the contrary or disregarding them entirely, spends considerable effort lambasting the "intentionally" component of the Defense proposed instruction as converting

Article 104 into a specific intent offense. This effort is fruitless. The Defense has said it once, and it will say it again: the “intentionally” component of the “knowingly and intentionally” requirement merely seeks to ensure that Article 104 does not impermissibly punish inadvertent, accidental, or negligent acts.

5. Much of the Government’s Response is dedicated to equating the “intentionally” aspect of the Defense’s proposed instruction to a specific intent requirement. *See* Government Response to Defense Motion for Specific Instructions: The Specification of Charge 1 [hereinafter Government Response], at 1 (“The Defense’s proposed instruction transforms the Government’s burden by requiring it to prove a specific intent to commit the charged offense, in contravention of the law, statutory text, and this Court’s previous rulings.”); *id.* at 2 (“The Government does not need to prove that the accused intended to give intelligence to the enemy through indirect means because Article 104 does not require specific intent.”); *id.* at 3 (“Any intention, purpose, design, or desire is only required under a specific intent and not under the general intent required for Article 104. Thus, the Government is not required to prove that the accused desired the specific result of the enemy’s receipt of intelligence.” (citations omitted)); *id.* (“The Defense’s proposed instruction requiring the Government to prove specific intent is improper. The Defense uses its request for instructions to raise anew its contention that, as charged in this case, Article 104 requires the Government to prove a specific intent to commit the offense.”). Perhaps the Government genuinely misunderstood the reason for the Defense’s inclusion of the “intentionally” component of the proposed “knowingly and intentionally” requirement. Perhaps the Government simply disregarded the reason for its inclusion and chose instead to argue an issue that was not raised by the Defense Motion. Either way, the Government’s effort on this score was a wasted one, since at no point in the Defense Motion did the Defense intimate that Article 104 was or should be a specific intent offense.

6. Rather, the Defense Motion clearly states the reason for including the “intentionally” component of the proposed “knowingly and intentionally” requirement: to prevent Article 104 from impermissibly punishing the inadvertent, mistaken, accidental, or negligent act. Footnote 2 of the Defense Motion stated with unmistakable clarity that:

Saying that an accused acted “intentionally” in this context is *not the same as saying an accused acted with any type of specific intent or motive* (e.g. intent to aid the enemy). *See* Appellate Exhibit LXXXI, at 3. Rather, the term “intentionally” here simply means that the accused intended to perform the act (i.e. intended to give intelligence to the enemy). In other words, it means that he did not act “inadvertently, accidentally, or negligently.” [*United States v.*] Olson, 20 C.M.R. [461.] 464 [(A.B.R. 1955)]; *see* Appellate Exhibit LXXXI, at 2, 4 (“A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently.”).

Defense Motion, at 6 n.2 (emphasis supplied). The Defense maintains in this Reply that if “knowingly and intentionally” is not the mens rea for the Article 104 offense, then this Court’s instructions will run afoul of the well-established proposition that Article 104 does not punish the inadvertent, accidental, or negligent act. *See United States v. Batchelor*, 22 C.M.R. 144, 157

(C.M.A. 1956); *Olson*, 20 C.M.R. at 464; Appellate Exhibit, LXXXI, at 2, 4 (“A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently.”).

7. Any of the loose conceptions of knowledge that the Government may wish would suffice – such as knowledge that an enemy might, could, or even would likely receive the intelligence – cannot prevent Article 104 from punishing the inadvertent, mistaken, accidental, or negligent act of an accused. For reasons discussed in the Defense Motion and in this Reply, *see* Part B, *supra*, this is especially true where, as here, an Internet-intelligence case is involved. The only way to ensure that Article 104 does not punish those who have acted inadvertently, accidentally, or negligently, *see* Appellate Exhibit LXXXI, at 2, 4, is to require the Government to prove actual knowledge on the part of the accused that he was giving intelligence to the enemy through indirect means. And the only sure way to require that actual knowledge be proven is to instruct the members that the accused must have knowingly and intentionally (i.e. intending to do the act or, conversely, not acting inadvertently, accidentally, or negligently) gave intelligence to the enemy through indirect means.

#### **B. The Government’s Instruction on Knowingly Would Impermissibly Allow Article 104 to Punish Negligent Acts**

8. Despite its best efforts to paint the Defense proposed instruction as illegitimate, the Government is the one who has proposed an impermissible instruction for Article 104. The definition of “knowingly” anticipated by the Government’s Response is far too lax; it would impermissibly allow Article 104 to punish inadvertent, accidental, or negligent acts. Accordingly, this Court should reject the Government’s definition of “knowingly” and adopt the Defense’s “knowingly and intentionally” standard.

9. In its response, the Government states that “a ‘knowingly’ standard simply requires awareness that a result is likely to follow, not a desire to effect that result.” Government Response, at 2. But simple awareness that a result is likely to follow cannot be the mens rea for an offense that cannot be consummated through inadvertent, accidental, or negligent acts. *See Batchelor*, 22 C.M.R. at 157; *Olson*, 20 C.M.R. at 464; Appellate Exhibit, LXXXI, at 2, 4 (“A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently.”). This is especially true for Internet-intelligence cases like this one.

10. Today, virtually everyone understands that information posted on a publicly accessible website can potentially be viewed by anyone with Internet access, including enemies of the United States. *See Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 851 (1997); *see also* Defense Motion, at 5. Certainly every Army analyst understands this fact. Therefore, under the Government’s understanding of “knowingly,” an Army analyst would certainly be aware that the enemy might, could, or would likely be able to access intelligence placed on the Internet. Thus, in the Government’s view, *anytime* an Army analyst placed *any* intelligence on the Internet, that analyst would have committed a capital offense, regardless of whether the analyst acted intentionally, inadvertently, accidentally, or negligently. This cannot be the proper understanding of Article 104’s “knowingly” requirement.

11. Indeed, the American Civil Liberties Union (ACLU) has indicated that it would be “brehtaking” if this were indeed the proper interpretation of Article 104:

**The Government's Overreach on Bradley Manning**

Yesterday the military judge overseeing the court martial of Pfc. Bradley Manning, who is accused of giving government documents to WikiLeaks, heard a defense motion to dismiss the charge of “Aiding the Enemy.” (She is expected to rule on the motion today.) The charge, which is akin to treason and is punishable by death, is separate from the main accusation against Manning — that he leaked sensitive documents to people unauthorized to receive them. The government’s inclusion of this charge raises enormous problems, and a conviction of Manning in these circumstances would be unconstitutional.

The key to the government’s case is this simple claim: that posting intelligence information to the internet aids Al Qaeda because Al Qaeda has access to the internet.

The implications of the government’s argument are breathtaking. To understand why, it helps to recall the experience of another soldier. In December of 2004, Defense Secretary Donald Rumsfeld held a town-hall style meeting for troops who were preparing to deploy to Iraq. Following his remarks, Rumsfeld was confronted by an Army specialist who complained about the inadequacy of the combat equipment provided by the military.

“Our vehicles are not armored,” said Specialist Thomas Wilson, an airplane mechanic with the Tennessee Army National Guard. “We’re digging pieces of rusted scrap metal and compromised ballistic glass that’s already been shot up . . . to put on our vehicles to take into combat. We do not have proper vehicles to carry with us north.”

The soldier’s question — and Rumsfeld’s now infamous response that “you go to war with the army you have, not the army you might want or wish to have” — were front-page news around the world. And while war cheerleaders like Rush Limbaugh accused Specialist Wilson of “near insubordination” for embarrassing the defense secretary in a public forum, there was no suggestion in serious quarters that he face punishment — much less prosecution — for his words. Yet the government’s decision to prosecute Manning for “Aiding the Enemy” threatens to make public comments like Wilson’s grounds for criminal prosecution. The government does not contend that Manning gave any information to Al Qaeda, or even that he intended that Al Qaeda receive it. Rather, it claims that Manning “indirectly” aided Al Qaeda by causing intelligence information to be posted on WikiLeaks’ website, knowing that Al Qaeda has access to the internet. Specifically, the government contends that Manning violated Article 104 of the Uniform Code of Military Justice, which provides that “any person who . . . gives intelligence to or communicates or corresponds with or holds any intercourse with the enemy, either directly or

indirectly; shall suffer death or such other punishment as a court-martial or military commission may direct.”

Article 104 is not limited to sensitive or classified information — it prohibits any unauthorized communication or contact with an enemy. So, if the government is right that a soldier “indirectly” aids the enemy when he posts information to which the enemy might have access, then the threat of criminal prosecution hangs over any service member who gives an interview to a reporter, writes a letter to the editor, or posts a blog to the internet.

For example, there are now more than a thousand enlisted military bloggers. According to Stars and Stripes, “Army officials . . . encourage troops to blog as long as it doesn’t break any operational security rules, and they see it as a good release for servicemembers.”

Are these bloggers aiding the enemy? Prior to Bradley Manning’s case, charging anyone with that crime in the absence of any allegation or evidence that he had intended to aid the enemy would have been inconceivable.

The crux of the government’s case against Manning — that he leaked sensitive documents without authorization — in no way depends on branding him a traitor. Indeed, some courts have held that leaks may be punished even if the leaker’s motive was purely patriotic. In its zeal to throw the book at Manning, the government has so overreached that its “success” would turn thousands of loyal soldiers into criminals.

Which brings us back to Specialist Wilson — and, for that matter, Donald Rumsfeld. Both men spoke openly about the vulnerability of U.S. forces in Iraq. Both men surely knew that the enemy would watch their exchange on television or read about it on the internet. The notion that Wilson and Rumsfeld broke the law by communicating this information to the media and thereby “indirectly” aiding the enemy is absurd — but no more so than the government’s contention that Bradley Manning did so.

See <http://www.aclu.org/blog/free-speech-national-security/governments-overreach-bradley-manning>.

12. This Court has held that Article 104 requires “actual knowledge” on the part of the accused that he was giving intelligence information to the enemy through indirect means. See Appellate Exhibit LXXXI, at 4 (“Article 104(2) requires *actual knowledge* by the accused that he was giving intelligence to the enemy.” (emphases supplied)); *id.* (“The accused must *actually know* that by giving intelligence to the 3<sup>rd</sup> party he was giving intelligence to the enemy through this indirect means.” (emphases supplied)). This Court did not hold that mere awareness that the enemy may be able to access the information or mere awareness that it would be likely that the enemy would access the information could suffice. In fact, by adopting an “actual knowledge” requirement this Court implicitly rejected any notion that bare awareness that a particular result



was likely could satisfy the mens rea of Article 104. *See id.* (“A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently.”). Other Article 104 case law fully supports this Court’s adoption of the “actual knowledge” requirement. *See Batchelor*, 22 C.M.R. at 157; *Olson*, 20 C.M.R. at 464.

13. Notwithstanding this Court’s ruling, the Government has attempted to water down beyond recognition the “actual knowledge” requirement adopted by this Court. Its Response focused primarily on unwarranted concerns that the Defense proposed instruction turned Article 104 into a specific intent offense. However, the Government also subtly sought to replace the “actual knowledge” mens rea with one requiring mere awareness of a likely result (i.e. constructive knowledge). This back door substitution cannot be permitted. Since this Court’s ruling requires that “[t]he accused must actually know that by giving intelligence to the 3<sup>rd</sup> party he was giving intelligence to the enemy through this indirect means[.]” Appellate Exhibit LXXXI, at 4, an accused cannot be found guilty of giving intelligence to the enemy where he gives intelligence to a third party with the mere awareness that the enemy might, could, or even would likely receive the intelligence. Actual knowledge that the accused was giving intelligence information to the enemy through indirect means is the requisite mens rea, *see id.*; mere awareness of a likely result is not. The Government’s proposed standard would impermissibly sweep inadvertent, accidental, and negligent acts under Article 104’s reach.

14. One must also recall that a prosecution such as this one has *never been maintained* in the history of the United States. This will be the first case in American history to consider whether causing information to be posted on the internet constitutes “indirectly” giving intelligence to the enemy. Since there is absolutely no precedent for a prosecution of this nature, this Court should err on the side of caution and ensure that panel members truly understand that “actual knowledge” cannot be satisfied by showing awareness of a possible, probable or likely result. Rather, the accused must have intended to give (as in, the act was volitional) intelligence to the enemy through the indirect means. While the accused did not have to *intend to aid* the enemy, he must have *intended to give* intelligence to the enemy.

15. Accordingly, this Court should reject that loose definition of “knowingly” and adopt the only sensible alternative: the “knowingly and intentionally” standard embodied in the Defense’s proposed instructions.

**C. A “Knowingly and Intentionally” Requirement is Supported by Offense 26 of the Military Commissions Act**

16. Finally, the Government’s attempt to distinguish Offense 26 of the Military Commissions Act from Article 104 is severely flawed in several respects. In its Response, the Government identified three ostensibly relevant differences between Offense 26 and Article 104: Offense 26 has a loyalty element absent from Article 104; Offense 26 uses the phrase “knowingly and intentionally” while Article 104 does not; and Offense 26 is entitled “Wrongfully Aiding the Enemy” while Article 104 is just entitled “Aiding the Enemy.” None of these three “distinctions” has even an ounce of merit.

17. First, the Government argues that Offense 26 is appreciably different from Article 104 because Offense 26 has a loyalty element absent from Article 104. The Government Response states: “In fact, Congress further heightened the requirements of Offense 26 in comparison to Article 104 by adding a loyalty element. See 10 U.S.C. § 950t(26) (requiring, among other elements, a “breach of an allegiance or duty to the United States”).” Government Response, at 4. This contention is nonsense. For one thing, as the Government itself acknowledges, Soldiers already owe a duty of loyalty to the United States. See *id.* at 4 n.3 (“[T]he Government notes that Soldiers . . . owe a duty of loyalty to the United States[.]”). This duty of loyalty is implicit in the UCMJ. For another thing, the loyalty element – whether explicit or implicit – has absolutely nothing to do with the mens rea of either Offense 26 or Article 104. The fact that Offense 26 makes one non-mens rea element explicit while Article 104 makes it implicit is irrelevant to the purpose for which the Defense compared the two offenses: to show that because Offense 26, which was modeled after and came from the same common law source as Article 104, has a “knowingly and intentionally” mens rea, Article 104 must have the same mens rea.<sup>1</sup>

18. Second, the Government attempts to distinguish Offense 26 from Article 104 by pointing out that Offense 26 contains a “knowingly and intentionally” mens rea while Article 104 does not. See Government Response, at 4 (“The Military Commissions Act comparison made by the Defense fails because Congress explicitly chose to add the “knowingly and intentionally” standard to Offense 26, yet the Drafters declined to change the language of Article 104 to include the “knowingly and intentionally” standard in both 2008 and 2012.”). While superficially appealing, this “distinction” breaks down upon closer examination. As was fully explained in the Defense Motion, Offense 26 does not create a new offense out of thin air. See Defense Motion, at 7. On the contrary, Section 950p(d) makes clear that the offenses currently listed in Section 950t, including Offense 26, are not new offenses, but are instead codifications of offenses traditionally triable by military commission. See 10 U.S.C. § 950p(d) (“The provisions of this subchapter codify offenses that have traditionally been triable by military commission. This chapter does not establish new crimes that did not exist before the date of the enactment of this subchapter[.]”).

19. Therefore, Congress did not simply make up the “knowingly and intentionally” mens rea for Offense 26; it had to come from somewhere. Like Article 104, Offense 26 is based on the common law of war offense of aiding the enemy, which has remained substantially unchanged

---

<sup>1</sup> The Government also relies on this loyalty element to portray as foolish the Defense’s suggestion that a terrorist could receive a friendlier mens rea standard under Offense 26 than a Soldier would receive under Article 104. See Government Response, at 4 n.3 (“[T]he Defense neglects to consider that the loyalty element, discussed *infra*, presumably would not apply to a terrorist because he would lack an ostensible allegiance or duty to the United States. Therefore, a terrorist would not be subject to Offense 26. Accordingly, the terrorist would not benefit from a “friendlier” mens rea than a Soldier charged with an Article 104 violation.”). However, the Government neglects to consider that the loyalty element upon which it relies can be satisfied by mere citizenship or resident alien status. See Manual for Military Commissions (MMC), Part IV, at 21 (2010 ed.) (“The requirement that conduct be wrongful for this crime necessitates that the accused owe allegiance or some duty to the United States of America. For example, citizenship, resident alien status, or a contractual relationship in or with the United States is sufficient to satisfy this requirement so long as the relationship existed at a time relevant to the offense alleged.”). Therefore, the Government is plainly mistaken that a terrorist would not be subject to Offense 26; a terrorist who is either a citizen of the United States or who has resident alien status would indeed be subject to Offense 26. Accordingly, in such a case, the terrorist *would* benefit from a friendlier mens rea than a Soldier charged with an Article 104 violation, provided, of course, that Article 104 does not require a “knowingly and intentionally” mens rea.

for the past 235 years. *See* Defense Motion, at 8. Given the similarities between Article 104 and Offense 26 and their shared common law roots, the unmistakable conclusion is that Article 104 and Offense 26 share the same “knowingly and intentionally” mens rea, derived from the common law of war offense that has remain unchanged for 235 years. *See id.*

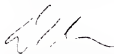
20. Finally, the Government seeks to distinguish Offense 26 from Article 104 by comparing the names of the two offenses. *See* Government Response, at 4 (“[T]he name of the offense cited by the Defense, ‘Wrongfully Aiding the Enemy,’ also indicates an increased standard. Here, the accused is charged with aiding the enemy, not ‘wrongfully’ aiding the enemy.”) This contention is barely deserving of a response. Article 104(2), the provision under which PFC Manning has been charged, punishes “[a]ny person who -- (2) *without proper authority*, knowingly harbors or protects or gives intelligence to, or communicates or corresponds with or holds any intercourse with the enemy, either directly or indirectly[.]” 10 U.S.C. § 904(2) (emphasis supplied). Likewise, the MMC offers the following explanation of the meaning of “wrongfully:” “The requirement that conduct be wrongful for the crime necessitates that the accused act *without proper authority*.” MMC, Part IV, at 21 (emphasis supplied). In this respect, then, the two offenses are exactly the same, notwithstanding the Government’s silly name game.

21. Therefore, as Offense 26 is obviously modeled after Article 104, derives from the same common law roots as Article 104, and cannot be effectively distinguished from Article 104, its “knowingly and intentionally” mens rea must also be contained in Article 104’s mens rea. Accordingly, Offense 26 offers yet another reason for this Court to adopt the “knowingly and intentionally” standard for the actual knowledge element of Article 104.

### CONCLUSION

22. For these reasons and those articulated in the Defense Motion, the Defense requests that this Court give the instructions requested in the Defense Motion and the Defense Requested Instruction for the Specification of Charge 1.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE REPLY TO  
GOVERNMENT RESPONSE TO  
DEFENSE REQUESTED  
INSTRUCTION:  
SPECIFICATIONS 4, 6, 8, 12 AND  
16 OF CHARGE II**

DATED: 11 July 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 920(c), requests this Court to give the instructions requested in the Defense Requested Instruction: Specifications 4, 6, 8, 12 and 16 of Charge II [hereinafter Defense Requested Instruction].

ARGUMENT

2. The Government objects to the language of various proposed instructions. That language comes virtually verbatim from the Federal Jury Instructions published by Matthew Bender & Co., Inc. Those jury instructions are attached in full with this motion, and the relevant language has been highlighted in yellow for ease of reference.

3. Specifically, the Government objects to the Defense's proposed stealing, purloining, and conversion instructions. With regards to the stealing instruction, the Government states that "[t]o 'steal' does not mean to take someone's property with the intent to deprive the owner of the value of that property." Government Response to Defense Requested Instruction: Specifications 4, 6, 8, 12 and 16 of Charge II [hereinafter Government Response], at 2 (emphasis in original). However, this is the precise definition provided by the attached jury instructions. See Federal Jury Instructions (attached), at 10.

4. Additionally, the Government offers a similar objection to the Defense's purloining instruction: "'purloin' is also not linked to the intent to permanently deprive the owner of the value of the property." Government Response, at 2 (emphasis in original). However, as the Government points out, to purloin is to steal with the added element of stealth. See *id.* ("See *United States v. Morissette*, 342 U.S. 246, 270 (1952) ('Stealing...is commonly used to denote any dishonest transaction whereby one obtains that which belongs to another, and deprives the owner of the rights and benefits of ownership, but may or may not involve the element of stealth

EXC 1X (199)  
APPELLATE EXHIBIT \_\_\_\_\_

Page \_\_\_\_\_ of Page(s)

(S 241)

usually attributed to the word purloin.'"))). Therefore, while the Federal Jury Instructions do not provide a definition of "purloin," the Defense maintains that its definition of purloin properly combines an acceptable definition of "steal," *see* Federal Jury Instructions (attached), at 10, with the extra element of stealth.

5. Finally, the Government also objects to the Defense's conversion instruction as follows: "in the 'conversion' instruction, the United States is not required to prove that the accused 'knew' that the property belonged to the United States, only that he knew that he [sic] property was not his." Government Response, at 2. However, the Federal Jury Instructions provide otherwise. *See* Federal Jury Instructions (attached), at 10.

6. Therefore, the Defense maintains that its requested instructions are entirely proper and that the Government's objections are without merit.

#### CONCLUSION

7. For these reasons, the Defense requests this Court to give the instructions requested in the Defense Requested Instruction.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

## ¶ 23A.01. Theft of Government Property (18 U.S.C. § 641)

## Instruction 23A-1

## The Indictment and the Statute

The indictment charges the defendant with stealing (*or embezzling or knowingly converting*) money or property belonging to the United States government. The indictment reads as follows:

## [Read Indictment]

The indictment charges the defendant with violating section 641 of Title 18 of the United States Code. That section provides in relevant part:

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys, or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof [shall be guilty of a crime].

---

Comment

The first two paragraphs of section 641 create different crimes with different elements: the first paragraph applies to the unlawful taking of government property, while the second concerns the unlawful possession of that property after it has been stolen. The Supreme Court has specifically held that a defendant may not be convicted under section 641 for both stealing and receiving the same property,<sup>1</sup> although the indictment may charge the defendant with both.<sup>2</sup>

The offense paragraphs of section 641 each provide for both a felony and a misdemeanor offense depending on the value of the property stolen. In its original version, the dividing line between the felony and misdemeanor offenses was set at \$100. That was increased to \$1,000 in 1996.<sup>3</sup>

<sup>1</sup> *Milanovich v. United States*, 365 U.S. 551, 554-55, 81 S. Ct. 728, 5 L. Ed. 2d 773 (1961).

<sup>2</sup> *United States v. Bauer*, 713 F.2d 71, 75 (4th Cir. 1983).

<sup>3</sup> Economic Espionage Act of 1996, P.L. No. 104-294, Title VI, § 606(a), 110 Stat. 3511 (1996).

## Instruction 23A-2

## Elements of the Offense

In order to prove the defendant guilty of stealing (*or* embezzling *or* knowingly converting) money or property belonging to the United States government, the government must prove each of the following elements beyond a reasonable doubt:

First, that the money or property described in the Indictment belonged to the United States government;

Second, that the defendant stole (*or* embezzled *or* knowingly converted) that property;

Third, that the defendant acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property; and

Fourth, that the value of the property was greater than \$1,000.

## Authority

**Fifth Circuit:** United States v. Dien Duc Huynh, 246 F.3d 734 (5th Cir. 2001); United States v. Aguilar, 967 F.2d 111 (5th Cir. 1992); Fifth Circuit Pattern Criminal Jury Instruction 2.33.

**Sixth Circuit:** United States v. McGahee, 257 F.3d 520 (6th Cir. 2001).

**Seventh Circuit:** United States v. Howard, 30 F.3d 871 (7th Cir. 1994); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641.

**Eighth Circuit:** Eighth Circuit Model Criminal Jury Instruction 6.18.641.

**Ninth Circuit:** United States v. Seaman, 18 F.3d 649 (9th Cir. 1994).

**Tenth Circuit:** United States v. Hill, 835 F.2d 759 (10th Cir. 1987).

**Eleventh Circuit:** United States v. McRee, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); United States v. Lanier, 920 F.2d 987 (11th Cir. 1991); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21.

## Comment

There is wide agreement on the elements of a violation of section 641, with some courts and circuit pattern instructions treating the value of the property as a separate element,<sup>1</sup> and others treating it as part of the first element.<sup>2</sup> Both

<sup>1</sup> United States v. McGahee, 257 F.3d 520, 528-29 (6th Cir. 2001); United States v. Seaman, 18 F.3d 649, 650 (9th Cir. 1994); United States v. McRee, 7 F.3d 976, 980 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); United States v. Medrano, 836 F.2d 861, 864 (5th Cir.), *cert. denied*.

formulations are equally acceptable; the former is recited here only because it simplifies instruction on the lesser included misdemeanor offense of stealing property with a value of \$1,000 or less.

The Ninth Circuit pattern instructions join the second and third elements as follows:

First, the defendant knowingly stole [money] [property of value] with the intention of depriving the owner of the use or benefit of the [money] [property];

Second, the [money] [property] belonged to the United States; and

Third, the value of the [money] [property] was more than \$1,000.<sup>3</sup>

In practice, the Ninth Circuit has approved both the version in the pattern instructions<sup>4</sup> and the recommended formulation.<sup>5</sup>

488 U.S. 818 (1988). See Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21.

<sup>2</sup> United States v. Dien Due Huynh, 246 F.3d 734, 745 (5th Cir. 2001); United States v. Howard, 30 F.3d 871, 875 (7th Cir. 1994); United States v. Burton, 871 F.2d 1566, 1570 (11th Cir. 1989); United States v. Hill, 835 F.2d 759, 762 n.2 (10th Cir. 1987). See Fifth Circuit Pattern Criminal Jury Instruction 2.33, Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641; Eighth Circuit Model Criminal Jury Instruction 6.18.641.

<sup>3</sup> Ninth Circuit Model Criminal Jury Instruction 8.31.

<sup>4</sup> United States v. Campbell, 42 F.3d 1199, 1204 (9th Cir. 1994), *cert. denied*, 514 U.S. 1091 (1995).

<sup>5</sup> United States v. Seaman, 18 F.3d 649, 650 (9th Cir. 1994).



## Instruction 23A-3

## First Element Money or Property Belonged to United States

The first element the government must prove beyond a reasonable doubt is that the money or property described in the Indictment belonged to the United States government.

To satisfy this element, the government must prove that [describe property] was a "thing of value of the United States." That means that at the time the property was allegedly stolen (or embezzled or knowingly converted) the United States government or an agency of the United States government had either title to, possession of or control over the property (or the property was made under contract for the United States).

(If appropriate, except in the Ninth Circuit: Property includes other things of value beside money and tangible objects. It also includes Intangible things like the value of an employee's time and services.)

Except when knowing conversion of the property is charged: The government is not required to prove that the defendant knew that the property was a "thing of value of the United States."

---

Comment

The requirement that the property allegedly stolen was a "thing of value of the United States" provides the link which establishes federal jurisdiction.<sup>1</sup> Instruction 23A-3 sets forth a basic charge for the usual case when it is alleged that the government owned the property. As discussed below, the phrase "thing of value of the United States" has been interpreted to apply to interests beyond ownership and possession, so the instruction will need to be revised to address those other interests when appropriate.

Despite some statements by the Ninth Circuit that the determination whether the property involved is a "thing of value of the United States" is a question of law,<sup>2</sup> it is strongly recommended that this issue be submitted to the jury. All of the circuit pattern instructions include a charge on this element,<sup>3</sup> and there has been no discussion of this issue outside the Ninth Circuit, suggesting that it is routinely charged to the jury. The better view is that this is a factual question

<sup>1</sup> United States v. Caselorente, 220 F.3d 727, 732 (6th Cir. 2000).

<sup>2</sup> United States v. Lawson, 925 F.2d 1207, 1209 (9th Cir. 1991); United States v. Eden, 659 F.2d 1376, 1378 (9th Cir. 1981), cert. denied, 455 U.S. 949 (1982).

<sup>3</sup> See Fifth Circuit Pattern Criminal Jury Instruction 2.33; Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641; Eighth Circuit Model Criminal Jury Instruction 6.18.641; Ninth Circuit Model Criminal Jury Instruction 8.31; Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21.

for the jury subject to review on appeal whether the interest alleged and found by the jury is sufficient as a matter of law.<sup>4</sup>

As noted above, the phrase "thing of value of the United States" has been interpreted to extend beyond actual ownership to include any situation in which the government has "title to, possession of or control over" the property.<sup>5</sup> The courts have tended to group these property interests into four categories: (1) when the government has clear ownership of the property; (2) when the government is the custodian or bailee of the property; (3) when a government employee or agent has possession of the property; and (4) when possession of the property has passed to an intermediary but the government retains supervision and control over the property.<sup>6</sup>

The first situation, when the government is alleged to have clear ownership of the property, is the simplest. Ownership of the property in question obviously satisfies the requirement that it be a "thing of value of the United States."<sup>7</sup> In addition to the garden variety items which would undoubtedly fall within this category without discussion, several types of property have been the subject of repeated discussion in the courts. Thus, it is now clear that natural resources on public lands are things of value,<sup>8</sup> as is merchandise for sale on military post exchanges.<sup>9</sup>

At least six courts of appeal have held that section 641 applies to intangible property such as government employee time and confidential information.<sup>10</sup> Only

<sup>4</sup> See *United States v. Lanier*, 920 F.2d 887, 896 (11th Cir. 1991).

<sup>5</sup> *United States v. Tailan*, 161 F.3d 591, 592 (9th Cir. 1998).

<sup>6</sup> See *United States v. Caselorente*, 220 F.3d 727, 732 (6th Cir. 2000).

<sup>7</sup> See, e.g., *United States v. Caselorente*, 220 F.3d 727, 732-33 (6th Cir. 2000) (government owned recyclables at time of conversion by defendant); *United States v. Faust*, 850 F.2d 575, 579 (9th Cir. 1988) (government had clear ownership interest in insurance check made out jointly to defendant and government).

<sup>8</sup> See *United States v. Newsome*, 322 F.3d 328, 333 (4th Cir. 2003) (trees); *United States v. McPhilomy*, 270 F.3d 1302, 1307-08 (10th Cir. 2001), *cert. denied*, 535 U.S. 966 (2002) (commercial grade stone); *United States v. Larson*, 110 F.3d 620, 624 (8th Cir. 1997) (fossils); *United States v. Campbell*, 42 F.3d 1199, 1203 (9th Cir. 1994), *cert. denied*, 514 U.S. 1091 (1995) (trees).

<sup>9</sup> *United States v. Tailan*, 161 F.3d 591, 592 (9th Cir. 1998); *United States v. Towns*, 842 F.2d 740, 741 (4th Cir.), *cert. denied*, 487 U.S. 1240 (1988); *United States v. Sanders*, 793 F.2d 107, 108-09 (5th Cir. 1986).

<sup>10</sup> *United States v. Collins*, 56 F.3d 1416, 1419-21 (D.C. Cir. 1995) (computer time and services); *United States v. Matzkin*, 14 F.3d 1014, 1020 (4th Cir. 1994) (confidential bid information); *United States v. Barger*, 931 F.2d 359, 368 (6th Cir. 1991) (confidential law enforcement information); *United States v. Croft*, 750 F.2d 1354, 1359-62 (7th Cir. 1984) (employee time); *United States v. Wilson*, 636 F.2d 225, 227-28 (8th Cir. 1980) (employee time); *United States v. Girard*, 601 F.2d 69, 71 (2d Cir.), *cert. denied*, 444 U.S. 871 (1979) (confidential law enforcement information). See also Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641 (Definition of Value); Eighth Circuit Model Criminal Jury Instruction 6.18.641. But see *Chappell v. United States*, 270 F.2d 274, 276 (9th Cir. 1959).

the Ninth Circuit disagrees, having held in an early case that section 641 does not apply to the theft of employee time.<sup>11</sup> As the District of Columbia Circuit explained, "Congress intended to enact a broad prohibition against the misappropriation of anything belonging to the government unrestrained by the fine and technical distinctions of the common law."<sup>12</sup> However, the defendant's actions must seriously interfere with the government's ownership rights. Thus, in the case just quoted, the court held that keeping personal documents on a government computer did not interfere with the government's use of the computer.<sup>13</sup>

A government check remains the property of the government until the check is received and deposited by the intended beneficiary.<sup>14</sup> Once the funds are deposited by the intended payee, however, title to the funds passes and is no longer property "of the United States."<sup>15</sup>

The government must be the owner of the property at the time of the alleged unlawful act. Once the government sells the property, the government becomes a creditor with respect to payment for that property and it is no longer property of the United States.<sup>16</sup> This rule is particularly important with respect to stolen government bonds. When bonds are purchased by a third party, they become the property of that purchaser, and are no longer property of the United States. However, if the bonds are subsequently stolen from the owner, under the applicable Treasury regulations the government will provide relief to the owner by replacing the bonds, and upon the granting of that relief, the stolen bonds become property of the United States.<sup>17</sup> As a result, the original theft of the bonds does not violate section 641, but retaining the bonds after relief has been granted to the owner is covered.<sup>18</sup> In that situation, the government must introduce evidence of when relief was granted, as the bonds became property "of the United States" at that time.<sup>19</sup>

<sup>11</sup> *Chappell v. United States*, 270 F.2d 274, 276 (9th Cir. 1959). See also *United States v. Tobias*, 836 F.2d 449, 451 (9th Cir. 1988) (dictum reaffirming Ninth Circuit's view on this subject).

<sup>12</sup> *United States v. Collins*, 56 F.3d 1416, 1419 (D.C. Cir. 1995).

<sup>13</sup> *Id.* at 1420-21. Note that the court affirmed defendant's conviction because he had also taken substantial quantities of office supplies in addition to the use of the computer. *Id.*

<sup>14</sup> *United States v. Gill*, 193 F.3d 802, 804 (4th Cir. 1999) (mother deposited sons' SSI disability check into unauthorized joint account over which son had no control, so title to funds never passed to intended beneficiary); *United States v. O'Kelley*, 701 F.2d 758, 760 (8th Cir.), cert. denied, 464 U.S. 838 (1983) (unendorsed check remains property of the United States even after receipt by beneficiary); *United States v. Forcellati*, 610 F.2d 25, 31 (1st Cir. 1979), cert. denied, 445 U.S. 944 (1980).

<sup>15</sup> *United States v. Howard*, 787 F. Supp. 769, 771 (S.D. Ohio 1992).

<sup>16</sup> *United States v. Gwin*, 839 F.2d 427, 429-30 (8th Cir. 1988).

<sup>17</sup> See 31 C.F.R. §§ 315.25, 315.28(b).

<sup>18</sup> *United States v. Stuart*, 22 F.3d 76, 80 (3d Cir. 1994); *United States v. Bauer*, 713 F.2d 71, 73 (4th Cir. 1983); *United States v. Carr*, 706 F.2d 1108, 1109-11 (11th Cir. 1983).

<sup>19</sup> *United States v. Stuart*, 22 F.3d 76, 80 (3d Cir. 1994).

The second form of interest that satisfies the "thing of value of the United States" standard is that at the time of the alleged taking, the government was the custodian or bailee of the property such that the government had possession of and control over the property.<sup>20</sup> For example, the government is the custodian of property seized or otherwise held as evidence in a criminal proceeding, so the government's possession of that evidence satisfies this element.<sup>21</sup>

The third category which constitutes a "thing of value of the United States" is property in the possession of a government employee or agent prior to conveyance to the government itself. Property which is in the possession of a government employee in his or her capacity as such is property of the United States.<sup>22</sup> Thus, a cashier at a military NCO club who stole the collective tip jar was found guilty of a violation of section 641 because at the time of the theft, she had possession of the funds in her role as an employee of the club.<sup>23</sup>

Non-employee agents of the government present a more complex problem. In that situation, the question to be determined is whether at the time of the theft the agent was a bailee of the property or a debtor of the government.<sup>24</sup> For example, in one case the defendant was an auctioneer contracted by the government to sell property repossessed from companies that had defaulted on government loans. Defendant sold the property as agreed, but then failed to turn the proceeds over to the government. The court of appeals noted that with respect to the property prior to the sale, the defendant was a consignee and the government retained ownership of the property. After the sale, however, under state law the sale of consigned property creates a debtor-creditor relationship between consignor and consignee with respect to the proceeds of the sale. As a result, the proceeds of the sale was not property of the United States at the time of the taking.<sup>25</sup>

The situation of an agent of the government must be distinguished from an agent of a third party who is holding money intended to be paid to the government. In that circumstance, the agent who converts the principal's funds

<sup>20</sup> See *United States v. Milton*, 8 F.3d 39, 42-43 (D.C. Cir. 1993), *cert. denied*, 513 U.S. 919 (1994) (money in account to be monitored and controlled by EEOC pending disbursement to aggrieved employees of the company involved was a bailment).

<sup>21</sup> *United States v. Perez*, 707 F.2d 359, 361-62 (8th Cir. 1983) (money introduced as exhibit at criminal trial); *United States v. Gordon*, 636 F.2d 886, 888-89 (5th Cir. 1981) (seized evidence in a drug case).

<sup>22</sup> *United States v. Caseslorente*, 220 F.3d 727, 732-33 (6th Cir. 2000) (proceeds of sale of recyclables was property of the United States); *United States v. Benefield*, 721 F.2d 128, 130 (4th Cir. 1983) (collective tip money at NCO club was government property until disbursement to staff).

<sup>23</sup> *United States v. Benefield*, 721 F.2d 128, 130 (4th Cir. 1983).

<sup>24</sup> *United States v. Lawson*, 925 F.2d 1207, 1209-10 (9th Cir. 1991).

<sup>25</sup> *Id.*

to his or her own use does not violate section 641 because the government has no legal interest in the funds prior to delivery by the agent.<sup>26</sup>

The fourth category of property interests, and certainly the most contentious, is when possession of the property has passed to an intermediary but the government retains supervision and control over the property. This arises in the common situation when the federal government sends block funds to a state agency or private entity for eventual disbursement to the intended third-party beneficiaries. In that circumstance, the courts are unanimously agreed that the property remains a thing of value of the United States after the transfer to the intermediary "so long as the government exercises supervision and control over the funds and their ultimate use."<sup>27</sup> Supervision and control requires a comprehensive set of regulations and contractual agreements governing the use and expenditure of the funds by the intermediary,<sup>28</sup> although it is not required that the government have a reversionary interest in the funds.<sup>29</sup> However, once the funds pass to an intended third-party beneficiary who has authority to expend it without federal supervision, it ceases to be property of the United States.<sup>30</sup>

Section 641 also applies to property "made under contract for the United States." Prosecutions involving this provision are rare, and tend to center on the

<sup>26</sup> *United States v. Klinger*, 61 F.3d 1234, 1238-41 (6th Cir. 1995) (customs broker converted checks intended to be paid as customs fees and duties); *United States v. Howard*, 30 F.3d 871, 875-76 (7th Cir. 1994) (government had only security interest in insurance proceeds paid directly to defendant); *United States v. Morris*, 541 F.2d 153, 154 (6th Cir. 1976) (funds of daycare center intended to pay for federal school lunch program); *United States v. Reed*, 851 F. Supp. 1296, 1311-12 (W.D. Ark. 1994), *aff'd*, 47 F.3d 288 (8th Cir. 1995) (attorney converted funds intended by client to pay income taxes).

<sup>27</sup> *United States v. McKay*, 274 F.3d 755, 758-59 (2d Cir. 2001), *cert. denied*, 535 U.S. 1028 (2002) (HUD section 8 funds). See *United States v. Lanier*, 920 F.2d 887, 896-97 (11th Cir. 1991) (SBA small vendor program); *United States v. Reynolds*, 919 F.2d 435, 437-38 (7th Cir. 1990), *cert. denied*, 499 U.S. 942 (1991) (HUD community block grant funds); *United States v. Foulks*, 905 F.2d 928, 930 (6th Cir. 1990) (FEMA emergency food program funds); *United States v. Litriello*, 866 F.2d 713, 714-15 (4th Cir. 1989) (federal employee health benefit plan funds); *United States v. Wheadon*, 794 F.2d 1277, 1284-85 (8th Cir. 1986), *cert. denied*, 479 U.S. 1093 (1987) (HUD grants to construct low-income housing); *United States v. Largo*, 775 F.2d 1099, 1101-02 (10th Cir. 1985), *cert. denied*, 474 U.S. 1105 (1986) (Bureau of Indian Affairs grants); *United States v. Von Stephens*, 774 F.2d 1411, 1413 (9th Cir. 1985) (AFDC vouchers); *United States v. McIntosh*, 655 F.2d 80, 84 (5th Cir. 1981), *cert. denied*, 455 U.S. 948 (1982) (FmHA loan funds prior to closing).

<sup>28</sup> *United States v. McKay*, 274 F.3d 755, 758-59 (2d Cir. 2001), *cert. denied*, 535 U.S. 1028 (2002).

<sup>29</sup> *United States v. Wheadon*, 794 F.2d 1277, 1285 (8th Cir. 1986), *cert. denied*, 479 U.S. 1093 (1987) (lack of reversionary interest is evidence that government had no property interest, but it is not decisive of the question).

<sup>30</sup> *United States v. Kristofic*, 847 F.2d 1295, 1297-99 (7th Cir. 1988) (even though SBA loan was made for specific purpose, once funds passed to small business, government had only a creditor relationship).

connection between the property and the federal government at the time of the theft. Thus, if the government had substantial supervisory control over the manufacture and handling of the items stolen, then this element has been held to be satisfied.<sup>31</sup> On the other hand, if the government did not have such supervision, then it is likely that this element will not be satisfied even if the government had nominal title under the contract.<sup>32</sup>

The last paragraph of the Instruction correctly states that there is no mens rea requirement to this element so that the government need not prove that the defendant knew that the property belonged to the United States, at least when the defendant is charged with stealing or embezzling.<sup>33</sup> When the defendant is charged with knowing conversion, knowledge that the property belonged to the United States is an element of the offense, so the last paragraph should be omitted in those cases.

The instruction does not include language requiring proof that the federal government suffered a loss as a result of the theft. In an early case, the Ninth Circuit stated that proof of loss is an "essential element" of an offense under section 641.<sup>34</sup> At least six other courts of appeal have since rejected that position.<sup>35</sup> Even the Ninth Circuit has retreated, stating more recently that the earlier case stands for the proposition that lack of proof of a loss is evidence that the property was not a "thing of value of the United States."<sup>36</sup> The Ninth Circuit pattern instruction makes no reference to this issue.<sup>37</sup>

<sup>31</sup> *United States v. Robie*, 199 F.3d 444, 452-53 (2d Cir. 1999) (misprinted stamps stolen from government printing contractor).

<sup>32</sup> *United States v. Hartec Enterprises, Inc.*, 967 F.2d 130, 133-34 (5th Cir. 1992) (nonconforming wire mesh screens sold by manufacturer for scrap).

<sup>33</sup> *United States v. Stuart*, 22 F.3d 76, 81 (3d Cir. 1994); *United States v. Sivils*, 960 F.2d 587, 595-96 (6th Cir.), *cert. denied*, 506 U.S. 843 (1992); *United States v. Bauer*, 713 F.2d 71, 73 n.4 (4th Cir. 1983); *United States v. Baker*, 693 F.2d 183, 186 (D.C. Cir. 1982); *United States v. Speir*, 564 F.2d 934, 938 (10th Cir. 1977) (en banc), *cert. denied*, 435 U.S. 927 (1978); *United States v. Jerniendy*, 544 F.2d 640, 641 (2d Cir. 1976), *cert. denied*, 430 U.S. 909 (1977); *United States v. Smith*, 489 F.2d 1330, 1332 (7th Cir. 1973), *cert. denied*, 416 U.S. 994 (1974); *Baker v. United States*, 429 F.2d 1278, 1279 (9th Cir. 1970), *cert. denied*, 400 U.S. 957 (1971).

<sup>34</sup> *United States v. Collins*, 464 F.2d 1163, 1165 (9th Cir. 1972).

<sup>35</sup> *United States v. Milton*, 8 F.3d 39, 44 (D.C. Cir. 1993), *cert. denied*, 513 U.S. 919 (1994); *United States v. Medrano*, 836 F.2d 861, 864 (5th Cir.), *cert. denied*, 488 U.S. 818 (1988); *United States v. Largo*, 775 F.2d 1099, 1101-02 (10th Cir. 1985), *cert. denied*, 474 U.S. 1105 (1986); *United States v. Bailey*, 734 F.2d 296, 301-05 (7th Cir.), *cert. denied*, 469 U.S. 931 (1984); *United States v. Santiago*, 729 F.2d 38, 40 (1st Cir. 1984); *United States v. Benefield*, 721 F.2d 128, 130 (4th Cir. 1983).

<sup>36</sup> *United States v. Faust*, 850 F.2d 575, 580 (9th Cir. 1988).

<sup>37</sup> See Ninth Circuit Model Criminal Jury Instruction 8.31.

## Instruction 23A-4

Second Element Defendant Stole or Embezzled Property<sup>1</sup>

The second element the government must prove beyond a reasonable doubt is that the defendant stole (*or embezzled or knowingly converted*) that property.

*If stealing is charged:* To steal money or property means to take someone else's money or property without the owner's consent with the intent to deprive the owner of the value of that money or property.

*If embezzlement is charged:* To embezzle money or property means to voluntarily and intentionally take or convert to one's own use money or property of another after that money or property lawfully came into the possession of the person taking it by virtue of some office, employment or position of trust.

*If conversion is charged:* To knowingly convert money or property means to use the property in an unauthorized manner in a way which seriously interfered with the government's right to use and control its own property, knowing that the property belonged to the United States, and knowing that such use was unauthorized.

## Authority

United States Supreme Court: *Morrisette v. United States*, 342 U.S. 246, 72 S. Ct. 240, 96 L. Ed. 2d 288 (1952).

Third Circuit: *United States v. Oliver*, 238 F.3d 471 (3d Cir. 2001).

Fourth Circuit: *United States v. Maisel*, 12 F.3d 423 (4th Cir. 1993); *United States v. Fogel*, 901 F.2d 23 (4th Cir.), *cert. denied*, 498 U.S. 939 (1990).

Fifth Circuit: *United States v. Aguilar*, 967 F.2d 106 (5th Cir. 1992).

Tenth Circuit: *United States v. Hill*, 835 F.2d 759 (10th Cir. 1987).

## Comment

More than a half century ago, in *Morrisette v. United States*,<sup>2</sup> the Supreme Court stated that "[t]o steal means to take away from one in lawful possession without right with the intention to keep wrongfully."<sup>3</sup> Instruction 23A-4 adopts a standard definition of stealing which is widely accepted.<sup>4</sup> Stealing includes

<sup>1</sup> The definition of knowing conversion is adapted from the charge of Judge Legg in *United States v. Maisel*, 12 F.3d 423 (4th Cir. 1993).

<sup>2</sup> 342 U.S. 246, 72 S. Ct. 240, 96 L. Ed. 2d 288 (1952).

<sup>3</sup> *Id.* at 271.

<sup>4</sup> *United States v. Aguilar*, 967 F.2d 106, 112 (5th Cir. 1992); *United States v. Hill*, 835 F.2d 759, 763 (10th Cir. 1987).

obtaining property by misrepresentation.<sup>5</sup> It also includes writing bad checks with no intention to pay.<sup>6</sup> The definition of embezzling is also a standard definition used throughout this Treatise.<sup>7</sup>

In discussing the meaning of stealing and the distinctions between the statutory terms embezzle, steal, purloin and knowingly convert, the *Morrisette* Court commented that "[p]robably every stealing is a conversion, but certainly not every knowing conversion is a stealing." The court continued:

Conversion . . . may be consummated without any intent to keep and without any wrongful taking, where the initial possession by the converter was entirely lawful. Conversion may include misuse or abuse of property. It may reach use in an unauthorized manner or to an unauthorized extent of property placed in one's custody for limited use. Money rightfully taken into one's custody may be converted without any intent to keep or embezzle it merely by commingling it with the custodian's own, if he was under a duty to keep it separate and intact. It is not difficult to think of intentional and knowing abuses and unauthorized uses of government property that might be knowing conversions but which could not be reached as embezzlement, stealing or purloining. Knowing conversion adds significantly to the range of protection of government property without interpreting it to punish unwitting conversions.<sup>8</sup>

Thus, in modern practice, the courts have tended to apply the knowing conversion provision in cases where defendant lawfully came into possession of the property but afterwards exercised dominion and control over the property knowing that he or she had no right to do so.<sup>9</sup> A common example is a government check mistakenly issued to defendant. In that situation, there is no question that defendant, the named payee, lawfully obtained possession of the check, but cashing the check knowing that he or she had no right to the underlying funds is a conversion.<sup>10</sup> The same is true for cashing social security checks sent to a recipient who has recently died.<sup>11</sup>

<sup>5</sup> *United States v. Oliver*, 238 F.3d 471 (3d Cir. 2001) (defendant was working full time at another job while receiving full disability benefits from his government job).

<sup>6</sup> *United States v. Aguilar*, 967 F.2d 106, 114-15 (5th Cir. 1992).

<sup>7</sup> See Instructions 24A-6 and 27A-5, *below*.

<sup>8</sup> 346 U.S. at 271-72.

<sup>9</sup> See *United States v. Maisel*, 12 F.3d 423, 425 (4th Cir. 1993); *United States v. Hill*, 835 F.2d 759, 764 (10th Cir. 1987). See also *United States v. Scott*, 789 F.2d 795, 798 (9th Cir. 1986) (*dictum*).

<sup>10</sup> *United States v. Irvin*, 67 F.3d 670, 672 (8th Cir. 1995) (clerical error in paycheck); *United States v. McRee*, 7 F.3d 976, 982 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994) (erroneous IRS refund).

<sup>11</sup> *United States v. Spear*, 734 F.2d 1, 2 (8th Cir. 1984); *United States v. Miller*, 200 F. Supp. 2d 616, 618-19 (S.D.W. Va. 2002).



**Instruction 23A-5**  
**Third Element Intent**

The third element the government must prove beyond a reasonable doubt is that the defendant acted knowingly and willfully with the intent to deprive the government of the use and benefit of its property.

To act knowingly means to act intentionally and voluntarily, and not because of ignorance, mistake, accident or carelessness.

To act willfully means to act with knowledge that one's conduct is unlawful and with the intent to do something the law forbids, that is to say with the bad purpose to disobey or disregard the law.

Whether the defendant acted knowingly and willfully may be proven by the defendant's conduct and by all of the circumstances surrounding the case.

**Authority**

**United States Supreme Court:** *Morrisette v. United States*, 342 U.S. 246, 72 S. Ct. 240, 96 L. Ed. 2d 288 (1952).

**Fourth Circuit:** *United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991).

**Fifth Circuit:** *United States v. Shackleford*, 677 F.2d 422 (5th Cir. 1982), *cert. denied*, 494 U.S. 899 (1983).

**Sixth Circuit:** *United States v. McGahee*, 257 F.3d 520 (6th Cir. 2001).

**Seventh Circuit:** *United States v. Croft*, 750 F.2d 1354 (7th Cir. 1984).

**Eighth Circuit:** *United States v. Wilson*, 636 F.2d 225 (8th Cir. 1980).

**Ninth Circuit:** *United States v. Scott*, 789 F.2d 795 (9th Cir. 1986); *United States v. Eden*, 659 F.2d 1376 (9th Cir. 1981), *cert. denied*, 455 U.S. 949 (1982).

**Eleventh Circuit:** *United States v. McRee*, 7 F.3d 976 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); *United States v. Burton*, 871 F.2d 1566 (11th Cir. 1989).

---

**Comment**

In *Morrisette v. United States*,<sup>1</sup> the Supreme Court specifically held that despite the lack of mens rea language in the statute, section 641 requires proof of intent.<sup>2</sup> Decided shortly after the end of World War II, *Morrisette* involved a defendant who was charged with a violation of section 641 after he removed

<sup>1</sup> 342 U.S. 246, 72 S. Ct. 240, 96 L. Ed. 2d 288 (1952).

<sup>2</sup> *Id.* at 260-61.

spent bomb casings from a former bombing range with the intention of melting the casings down for scrap. At trial, defendant argued that he believed the casings were abandoned, and that he had no intent to deprive the government of its property. The trial court rejected that argument, holding that abandonment of the property is not a defense because the statute does not require an intent to steal. In a decision with wide-ranging implications beyond section 641, the Supreme Court decided otherwise, and reversed defendant's conviction.

Even though the statute contains no stated intent element, the Court rejected the suggestion that the "mere omission from a criminal enactment of any mention of criminal intent [should be interpreted] as dispensing with it."<sup>3</sup> While certain regulatory offenses may dispense with an intent element, "stealing, larceny and its variants and equivalents, were among the earliest offenses known," and courts have always "consistently retained the requirement of intent in larceny-type offenses."<sup>4</sup>

Following *Morrisette*, it is now universally agreed that the defendant must act knowingly and willfully and with the specific intent to deprive the government of the use and benefit of its property.<sup>5</sup> Because of this requirement, several defenses may arise which tend to negate the necessary specific intent. In addition to abandonment of the property, which the *Morrisette* Court recognized as a potential defense,<sup>6</sup> a defendant would be entitled to an instruction on good faith,<sup>7</sup> or to the related defense that he or she had a claim of right to the property,<sup>8</sup> when the evidence supports such a defense.

<sup>3</sup> *Id.* at 250.

<sup>4</sup> *Id.* at 260-61.

<sup>5</sup> *United States v. McGahee*, 257 F.3d 520, 531 (6th Cir. 2001); *United States v. McRee*, 7 F.3d 976, 983 (11th Cir. 1993), *cert. denied*, 511 U.S. 1074 (1994); *United States v. Fowler*, 932 F.2d 306, 316-17 (4th Cir. 1991); *United States v. Scott*, 789 F.2d 795, 798 (9th Cir. 1986); *United States v. Croft*, 750 F.2d 1354, 1362-63 (7th Cir. 1984); *United States v. Shackelford*, 677 F.2d 422, 425 (5th Cir. 1982), *cert. denied*, 494 U.S. 899 (1983); *United States v. Wilson*, 636 F.2d 225, 228 (8th Cir. 1980).

<sup>6</sup> 342 U.S. at 271. See *United States v. Shackelford*, 677 F.2d 422, 425 (5th Cir. 1982), *cert. denied*, 494 U.S. 899 (1983); *United States v. Bess*, 593 F.2d 749, 752 (6th Cir. 1979).

<sup>7</sup> *United States v. Fowler*, 932 F.2d 306, 317-18 (4th Cir. 1991) (approving good faith instruction).

<sup>8</sup> *United States v. Heathershaw*, 81 F.3d 765, 768-69 (8th Cir. 1996); *United States v. Hill*, 835 F.2d 759, 768-69 (8th Cir. 1996).

## Instruction 23A-6

## Fourth Element Value of Property

The fourth and final element the government must prove beyond a reasonable doubt is that the value of the property stolen (or embezzled or knowingly converted) was greater than \$1,000.

The word "value" means face, par or market value, or cost price, either wholesale or retail, whichever is greater. "Market value" means the price a willing buyer would pay a willing seller at the time the property was stolen.

*(If appropriate: In determining the value of the property stolen, you may consider the aggregate or total value of the property referred to in the Indictment. If you find that the aggregate value is \$1,000 or less, then you must find the defendant not guilty. On the other hand, if the you find that the aggregate value to be greater than \$1,000, then this element is satisfied.)*

## Authority

**Second Circuit:** United States v. Robie, 166 F.3d 444 (2d Cir. 1999).

**Fifth Circuit:** United States v. Medrano, 836 F.2d 861, 864-65 (5th Cir.), *cert. denied*, 488 U.S. 818 (1988); United States v. Jeter, 775 F.2d 670, 680 (6th Cir. 1985), *cert. denied*, 475 U.S. 1142 (1986); Fifth Circuit Pattern Criminal Jury Instruction 2.32.

**Seventh Circuit:** United States v. Oberhardt, 887 F.2d 790 (7th Cir. 1989); United States v. Watkins, 709 F.2d 475 (7th Cir. 1983); Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641 (Definition of Value).

**Eighth Circuit:** Eighth Circuit Model Criminal Jury Instruction 6.18.64.1.

**Ninth Circuit:** United States v. Bigelow, 728 F.2d 412, 414 (9th Cir.), *cert. denied*, 469 U.S. 868 (1984).

**Tenth Circuit:** United States v. McPhilomy, 270 F.3d 1302 (10th Cir. 2001), *cert. denied*, 535 U.S. 966 (2002); United States v. Alberico, 604 F.2d 1315 (10th Cir.), *cert. denied*, 444 U.S. 992 (1979).

**Eleventh Circuit:** United States v. Langston, 903 F.2d 1510 (11th Cir. 1990); Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21.

## Comment

The term "value" is specifically defined in section 641 to mean "face, par or market value, or cost price, either wholesale or retail, whichever is greater."<sup>1</sup> Numerous courts have upheld instructions quoting that definition verbatim.<sup>2</sup> The

<sup>1</sup> 18 U.S.C. § 641.

<sup>2</sup> See, e.g., United States v. McPhilomy, 270 F.3d 1302, 1311 (10th Cir. 2001), *cert. denied*.

recommended instruction goes slightly further, including a standard definition of market value as well.<sup>3</sup>

The broad definition of value allows the jury to choose among several different methods of valuation, choosing the greatest value among those possibilities. Thus, the face value of the property is always relevant, even when the defendant could not have obtained that amount by selling it.<sup>4</sup> The courts are agreed that the value of the property in a "thieves' market" is an acceptable measure of value.<sup>5</sup> This means that the amount that defendant received for the property is evidence of its value.<sup>6</sup> This is so even when the commercial value of the property or the price at which the government would have sold the property is lower than the amount received by defendant.<sup>7</sup> Evidence of what the defendant believed he or she could get for the property, usually evidenced by an offering price, is also a legitimate measure of value for the purposes of this element.<sup>8</sup>

Valuation is measured as of the time of the unlawful act committed by defendant. Thus, if defendant is charged with stealing the property, then value is measured at the time of the theft.<sup>9</sup> On the other hand, if defendant is charged with concealing or retaining the property, then value can be measured at any time during defendant's possession.<sup>10</sup>

535 U.S. 966 (2002); *United States v. Robie*, 166 F.3d 444, 449 (2d Cir. 1999); *United States v. Watkins*, 709 F.2d 475, 480 (7th Cir. 1983). See Fifth Circuit Pattern Criminal Jury Instruction 2.32; Eighth Circuit Model Criminal Jury Instruction 6.18.641; Eleventh Circuit Pattern Criminal Jury Instructions, Offense Instruction 21.

<sup>3</sup> See Seventh Circuit Pattern Criminal Jury Instruction to 18 U.S.C. § 641 (Definition of Value). See also *United States v. Brookins*, 52 F.3d 615, 619 (7th Cir. 1995) (approving this language in a case involving 18 U.S.C. § 659).

<sup>4</sup> *United States v. Albericci*, 604 F.2d 1315, 1321-22 (10th Cir.), *cert. denied*, 444 U.S. 992 (1979) (face value of checks made out to military post was legitimate measure of value even though defendant could not have obtained that value).

<sup>5</sup> *United States v. Robie*, 166 F.3d 444, 451 (2d Cir. 1999); *United States v. Langston*, 903 F.2d 1510, 1514 (11th Cir. 1990); *United States v. Oberhardt*, 887 F.2d 790, 792-93 (7th Cir. 1989); *United States v. Jeter*, 775 F.2d 670, 680 (6th Cir. 1985), *cert. denied*, 475 U.S. 1142 (1986); *United States v. Bigelow*, 728 F.2d 412, 414 (9th Cir.), *cert. denied*, 469 U.S. 868 (1984); *United States v. Gordon*, 638 F.2d 886, 889 (5th Cir.), *cert. denied*, 452 U.S. 909 (1981).

<sup>6</sup> *United States v. McPhilly*, 270 F.3d 1302, 1311 (10th Cir. 2001), *cert. denied*, 535 U.S. 966 (2002); *United States v. Medrano*, 836 F.2d 861, 864-65 (5th Cir.), *cert. denied*, 488 U.S. 818 (1988); *United States v. Jeter*, 775 F.2d 670, 680 (6th Cir. 1985), *cert. denied*, 475 U.S. 1142 (1986); *United States v. Bigelow*, 728 F.2d 412, 413-14 (9th Cir.), *cert. denied*, 469 U.S. 868 (1984).

<sup>7</sup> *United States v. McPhilly*, 270 F.3d 1302, 1311 (10th Cir. 2001), *cert. denied*, 535 U.S. 966 (2002); *United States v. Oberhardt*, 887 F.2d 790, 792-93 (7th Cir. 1989).

<sup>8</sup> *United States v. Robie*, 166 F.3d 444, 449 (2d Cir. 1999).

<sup>9</sup> *United States v. Robie*, 166 F.3d 444, 449 (2d Cir. 1999).

<sup>10</sup> *United States v. Kramer*, 289 F.2d 909, 921 (2d Cir. 1961).

Finally, the instruction contains optional language allowing the jury to aggregate the value of stolen items charged in the indictment to reach the \$1,000 level.<sup>11</sup> If there is a legitimate question as to whether the value of the stolen property exceeded \$1,000, the court should give a lesser included offense instruction allowing the jury to consider whether defendant is guilty of the misdemeanor offense of theft of government property less than \$1,000.<sup>12</sup>

<sup>11</sup> Identity Theft Penalty Enhancement Act of 2004, P.L. No. 108-275, § 4118 Stat. 831 (2004)(effective July 15, 2004). Even before this amendment of section 641 specifically allowing aggregation, several courts had reached the same result. See *United States v. Smith*, 373 F.3d 561, 565-68 (4th Cir. 2004); *United States v. Robie*, 166 F.3d 444, 449 (2d Cir. 1999).

<sup>12</sup> See Committee Comment to Seventh Circuit Pattern Criminal Jury Instruction 18 U.S.C. § 641; Notes on Use to Eighth Circuit Model Criminal Jury Instruction 6.18.641 n.4; Eleventh Circuit Pattern Criminal Jury Instructions, Annotations and Comment to Offense Instruction 21.

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE REPLY TO  
GOVERNMENT RESPONSE TO  
DEFENSE REQUESTED  
INSTRUCTION:**

**SPECIFICATIONS 2, 3, 5, 7, 9, 10,  
11 AND 15 OF CHARGE II**

DATED: 11 July 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 920(c), requests this Court to give the instructions requested in the Defense Requested Instruction: Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II [hereinafter Defense Requested Instruction].

ARGUMENT

2. The Government Response specifically objected to particular instructions in the Defense Requested Instruction. For simplicity's sake, this Reply states the Defense's responses in similar fashion.

**A. Information Related to the National Defense**

3. The Government's assertion that the Defense Requested Instruction for this element "is an inaccurate characterization of the law" is unfounded. Government Response to Defense Requested Instruction: Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II [hereinafter Government Response], at 2.

4. The first sentence of the instruction for this element that was objected to by the Government ("However, only information of the type which, if disclosed, could threaten the national security of the United States meets the definition of information "related to the national defense" for the purpose of this section.") is based on the instructions approved by the Fourth Circuit in *United States v. Morison*, 844 F.2d 1057, 1071 (1988), and *United States v. Dedeyan*, 584 F.2d 36, 39-40 (1978), and the instruction given by the Court in *United States v. Rosen*, 445 F. Supp. 2d 602, 622 (E.D. Va. 2006).

5. The next two sentences of this instruction ("The connection must not be a strained one or an arbitrary one. The relationship must be reasonable and direct.") are taken verbatim from the

instruction approved by the United States Supreme Court in *Gorin v. United States*, 312 U.S. 19, 31 (1941).

6. The Government is correct that the remainder of that paragraph in the proposed instruction is based on language used by Judge Wilkinson in *Morison*, 844 F.2d at 1082, and by Justice Brennan in *New York Times Co. v. United States*, 403 U.S. 713, 726-27 (1971). However, the Defense maintains that this language is necessary to cure any unconstitutional vagueness, substantial overbreadth, or First Amendment implications that would result if the phrase "relating to the national defense" is defined as the Government has defined it. See Appellate Exhibit LCCCVIII, at 2-8.

7. With respect to the Defense Requested Instruction regarding the necessity of the Government showing that the information was closely held, the Defense maintains that, in order to cure any unconstitutional vagueness and substantial overbreadth in the phrase "relating to the national defense," the Government must prove that the information was classified. *Id.* at 8. Moreover, in Specifications 3, 5, 7, 9, 10 and 15 of Charge II, the Government has alleged that the information was classified. See Charge Sheet. The Government must therefore prove that this information was in fact classified.

**B. Information Could be Used to the Injury of the United States**

8. With regards to the Government's objections to the Defense Requested Instructions for the "could be used to the injury of the United States" element, the Defense maintains its position that the phrase "could be used" cannot be given its literal meaning. See Appellate Exhibit CLXIV, at 5-6. If the phrase "could be used" is given its literal meaning, so that a remote, hypothetical, speculative, far-fetched or fanciful possibility of injury to the United States would suffice, Section 793(e) would likely be unconstitutionally vague, especially when combined with the other borderline vague terms in that section. See Appellate Exhibit LCCCVII, at 2-7; Appellate Exhibit CLXIV, at 5-6. While the Defense concedes that the legitimate danger standard articulated in the Defense Requested Instruction has not yet been used in a court instruction, some safeguard must be put in place to prevent this element from covering the remote, hypothetical, speculative, far-fetched or fanciful possibility of injury to the United States.

CONCLUSION

9. For these reasons, the Defense requests this Court to give the instructions requested in the Defense Requested Instruction.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE REPLY TO  
GOVERNMENT RESPONSE TO  
DEFENSE REQUESTED  
INSTRUCTION:  
SPECIFICATIONS 13 AND 14 OF  
CHARGE II**

DATED: 11 July 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 920(c), requests this Court to give the instructions requested in the Defense Requested Instruction: Specifications 13 and 14 of Charge II [hereinafter Defense Requested Instruction].

ARGUMENT

2. The Government objects to the language of various proposed instructions. That language comes virtually verbatim from the Federal Jury Instructions published by Matthew Bender & Co., Inc. Those jury instructions are attached in full with this motion, and the relevant language has been highlighted in yellow for ease of reference.

3. The Defense Reply to the Government Response to the Defense Renewed Motion to Dismiss Specifications 13 and 14 of Charge II covers all responses to the Government's objections to the Defense's proposed instruction on the "exceeds authorized access" element.

CONCLUSION

4. For these reasons, the Defense requests this Court to give the instructions requested in the Defense Requested Instruction.

Respectfully submitted,

  
DAVID EDWARD COOMBS  
Civilian Defense Counsel



## ¶ 40A.01. Obtaining Protected or Restricted Information (18 U.S.C. § 1030(a)(1))

## Instruction 40A-1

## The Indictment and the Statute

The indictment charges that the defendant knowingly accessed a computer, either without authorization or outside the scope of authorization, and by means of such conduct obtained [state information named in indictment] and willfully communicated (*or delivered or transmitted*) that information to another person who was not entitled to receive it.

The indictment reads as follows:

## [Read Indictment]

The relevant statute on this subject is section 1030(a)(1) of Title 18 of the United States Code. It provides:

Whoever having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government . . . to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it [shall be guilty of a crime].

---

Comment

Section 1030(a)(1) was substantially revised by the Economic Espionage Act of 1996.<sup>1</sup> Prior to the 1996 Act, the focus of this section was to prevent the knowing accessing of a computer without proper authorization for the purpose  
(Text continued on page 40A-5)

<sup>1</sup> Pub. L. No. 104-294, § 201(1)(A), 110 Stat. 3501 (1996).

of obtaining protected information. As the legislative history indicated, the statute was analogous to "breaking and entering" rather than using the computer to commit an offense: Congress' analogy is that section 1030 is similar to burglarizing a home rather than using a gun to threaten the inhabitants.<sup>2</sup>

The 1996 Act refocuses the proscribed conduct by incorporating an additional element that the defendant must willfully communicate, deliver, or transmit the misappropriated information. Extending Congress' analogy, the statute as revised requires that the defendant trade in the stolen goods after burglarizing the home.

<sup>2</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 4 (1984).

## Instruction 40A-2

## Purpose of the Statute

Congress passed this law providing criminal penalties for certain abuses of computer technology in response to society's increased dependence on computers and the criminal element's enlarged capacity to carry out computer frauds.

---

Authority

H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 4 (1984).

---

Comment

Prior to the passage of 18 U.S.C. § 1030, no specific federal legislation governed the area of computer-related crime. The only relevant federal statutes were those governing mail and wire fraud.<sup>1</sup> Accordingly, the success of a prosecution for "computer fraud" rested upon fitting the alleged wrongdoing into the language of either of those two laws.

For example, in *United States v. Seidlitz*,<sup>2</sup> the owner of a computer company stole the confidential software of a previous employer by accessing the software from a remote computer terminal. As the House Report points out, "[h]ad the defendant not made two of the fifty access calls across State lines—there would have been no basis for Federal prosecution."<sup>3</sup>

The inadequacy of the criminal law to deal with computer-related fraud became apparent to Congress. First, the use of the mails or the use of interstate wires was not integral to the success of a computer fraud scheme. Moreover, conventional legal doctrine was largely inapplicable to computer crime, for "much of

<sup>1</sup> 18 U.S.C. §§ 1341, 1343. See Chapter 44, *Mail, Wire and Bank Fraud*.

<sup>2</sup> 589 F.2d 152 (4th Cir. 1978), *cert. denied*, 441 U.S. 922 (1979). See also *United States v. Giovengo*, 637 F.2d 941 (3d Cir. 1980), *cert. denied*, 450 U.S. 1032 (1981) (communication with out-of-state computer was necessary for successful execution of wire fraud scheme); *United States v. Computer Sciences Corporation*, 511 F. Supp. 1125 (E.D. Va. 1981), *rev'd and remanded*, 689 F.2d 1181 (4th Cir. 1982), *cert. denied*, 459 U.S. 1105 (1983) (fraud theory based on transmission of computer signals over interstate wires).

<sup>3</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 6 (1984).

the property involved does not fit well into categories of property subject to abuse or theft; a program, for example, may exist only in the form of magnetic impulses. Also, when a program of substantial commercial value is misappropriated, the person from whom it is stolen almost always remains in possession of the original."<sup>4</sup>

Faced with the crucial role that computer technology plays in the day-to-day operation of both the public and private sectors, the heightened sophistication of criminals in the computer crime area, and the enormity of the losses incurred as a result of computer fraud, Congress decided to provide "a clearer statement of proscribed activity" to the law enforcement community, owners and operators of computers, and those who might be tempted to commit crimes by unauthorized access to computers.<sup>5</sup>

<sup>4</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. at 9 (1984).

<sup>5</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. at 6-9 (1984). The legislative history indicates that the statute is not limited to highly sophisticated criminals. So-called "hackers" are also within the purview of the statutory language. *Id.* at 10-11.

## Instruction 40A-3

## Elements of the Offense

In order to prove the defendant guilty of the crime charged in the indictment, the government must establish each of the following elements beyond a reasonable doubt:

First, that without authorization, the defendant accessed a computer (*or* accessed a computer with authorization, but exceeded his authority in accessing the information in question);

Second, that the defendant knowingly accessed that computer;

Third, that the defendant obtained information protected against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, with the intent to use such information against the interests of the United States; and

Fourth, that the defendant willfully communicated (*or* delivered *or* transmitted *or* caused to be communicated, delivered, or transmitted *or* attempted to communicate, deliver, transmit) the information obtained to any person not entitled to receive it (*or* willfully retained that information and failed to deliver it to the officer or employee of the United States entitled to receive it).

---

Authority

18 U.S.C. § 1030(a)(1).

---

Comment

The four elements of the offense generally focus on the defendant's behavior, rather than on whether the device at issue is a computer which will rarely be in issue. However, because the statute provides a specific definition of a computer,<sup>1</sup> the jury is asked to decide whether the device in question is a computer in connection with the first element of the offense.<sup>2</sup> The fourth element was added by the Economic Espionage Act of 1996.<sup>3</sup>

<sup>1</sup> See 18 U.S.C. § 1030(e)(1).

<sup>2</sup> See Comment to Instruction 40A-4, *infra*.

<sup>3</sup> Pub. L. No. 104-294, § 201(1)(A)(vi), 110 Stat. 3501 (1996).

Note that there is no interstate commerce or monetary threshold element in 18 U.S.C. §§ 1030(a)(1), (2), (3) or (4), although Congress proposed both in earlier versions of the bill.<sup>4</sup> There are such requirements in section 1030(a)(5) cases.<sup>5</sup>

The Ninth Circuit pattern instructions contain a slightly different formulation:

First, the defendant knowingly [accessed without authorization] [exceeded authorized access to] a computer;

Second, by [accessing without authorization] [exceeding authorized access to] a computer, the defendant obtained [information that had been determined by the United States Government to require protection against disclosure for reasons of national defense or foreign relations] [data regarding the design, manufacture or use of atomic weapons];

Third, the defendant acted with the intent or reason to believe that the information or data obtained could be used to the injury of the United States or to the benefit of a foreign nation; and

Fourth, the defendant willfully [[caused to be] [[communicated] [delivered] [transmitted]]] to any person not entitled to receive it] [retained and failed to deliver to an officer or employee of the United States entitled to receive it] such information or data.<sup>5.1</sup>

<sup>4</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 20-22 (1984).

<sup>5</sup> See ¶ 40A.05, *below*.

<sup>5.1</sup> Ninth Circuit Model Criminal Jury Instruction 8.77.

## Instruction 40A-4

## First Element—Unauthorized Access of a Computer

The first element that the government must prove beyond a reasonable doubt is that the defendant accessed a computer without authorization, (or accessed a computer with authorization, but exceeded his authority in accessing the information in question).

As defined in the statute, a "computer" means "an electronic, magnetic, optical, electromechanical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." The statute makes clear that the term "computer" does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar devices.

*(If applicable:* In this case, the government charges that the defendant, while authorized to access the computer, exceeded his authority in accessing the information in question. Under the statute, this requires the government to prove beyond a reasonable doubt that the defendant had access to the computer, and used that access to obtain or alter information in the computer that the defendant was not entitled to obtain or alter.)

---

Authority

18 U.S.C. § 1030(e).

H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 22 (1984).

---

Comment

Instruction 40A-4 is intended to establish both components of the first element of the offense: that the device in question was a computer, and that the defendant accessed that device without authorization.

According to the House Report, defining the word "computer" has been problematic from the early days of computer crime legislation, given the rapid

technological advances in computer technology.<sup>1</sup> The original version of 18 U.S.C. § 1030 contained a dictionary definition of "computer." The more specific definition found in section 1030(e)(1) was chosen in order to avoid constitutional attacks upon the statute for vagueness.<sup>2</sup>

Sections 1030(a)(1), (2) and (4) contain specific language making the provision applicable to one who exceeds authorized access to a computer in addition to one who accesses the computer without any authorization. Accordingly, the last optional paragraph of the instruction contains language for those cases in which it is alleged that the defendant exceeded authorized access.<sup>3</sup> This paragraph basically tracks the statutory language.<sup>4</sup>

In *United States v. Morris*,<sup>5</sup> a case involving a previous version of section 1030(a)(5), the Second Circuit held that it is unnecessary to provide the jury with a definition of "authorization," because the word is of common usage and does not have an ambiguous meaning, thereby precluding the need for an instruction on its definition.<sup>6</sup> In those cases where a definition of authorization may be helpful, the following, adapted from the 1994 amendment to subsection (a)(5), is recommended:

This element requires that the government prove that the defendant's access of the computer was unauthorized. This means that the defendant accessed the computer without the permission of the person or entity who owns or is responsible for the computer.

<sup>1</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 23 (1984), citing Computer Systems Protection Act of 1979, S. 240; Hearing before the Subcommittee on Criminal Justice of the Senate Committee on the Judiciary, 96th Cong., 2d Sess. 8 (1980).

<sup>2</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 23 (1984).

<sup>3</sup> See, e.g., *United States v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir. 1997).

<sup>4</sup> See 18 U.S.C. § 1030(e)(6).

<sup>5</sup> 928 F.2d 504 (2d Cir.), cert. denied, 502 U.S. 817 (1991).

<sup>6</sup> 928 F.2d at 511.



## Instruction 40A-5

Second Element—Knowing Conduct<sup>1</sup>

The second element that the government must prove beyond a reasonable doubt is that the defendant acted knowingly in accessing the computer without authorization (*or* outside the scope of his authority).

“Knowingly” means to act voluntarily and deliberately, rather than mistakenly or inadvertently.

The question of whether a person acted knowingly is a question of fact for you to determine, like any other fact question. The question involves one’s state of mind.

Direct proof of knowledge is almost never available. It would be a rare case where it could be shown that a person wrote or stated that as of a given time in the past he committed an act with knowledge. Such proof is not required. The ultimate fact of knowledge, though subjective, may be established by circumstantial evidence, based upon a person’s outward manifestations, his words, his conduct, his acts and all the surrounding circumstances disclosed by the evidence and the rational or logical inferences that may be drawn from them.

Circumstantial evidence, if believed, is of no less value than direct evidence. In either case, the essential elements of the crime charged must be established beyond a reasonable doubt.

As a practical matter, then, in order to sustain the charges against the defendant, the government must establish beyond a reasonable doubt that he knew that his accessing of a computer was unauthorized (*or* that he knew his accessing of a computer was outside the scope of authorization granted).

The government can also meet its burden of showing that a defendant had actual knowledge of the accessing of a computer without authorization if it establishes beyond a reasonable doubt that he acted with deliberate disregard of whether he was so authorized, or with a conscious purpose to avoid learning the nature and scope of his authorization. Alternatively, the government may satisfy its burden of proving knowledge by establishing beyond a reasonable doubt that the defendant acted with an awareness of the high probability that he was acting without authorization, unless the defendant actually believed that he had authorization to access a computer in the manner described in the indictment. This guilty knowledge, however, cannot be established by demonstrating that the defendant was merely negligent or foolish.

<sup>1</sup> Adapted from the charges of Judge Weinfeld in *United States v. Ranney*, 82 Cr. 771 (S.D.N.Y. 1983), and *United States v. Della Rocca*, 72 Cr. 217 (S.D.N.Y. 1972).

To conclude on this element, if you find that the defendant did not know he was acting without authorization, then you should find the defendant not guilty.

However, if you find that the government has established beyond a reasonable doubt not only the first element, namely, the accessing of a computer, but also this second element, that the defendant acted knowingly without authorization, and if the government also establishes the third element, as to which I am about to instruct you, then you have a sufficient basis upon which to convict the defendant.

---

#### Authority

18 U.S.C. § 1030(a)(1).

---

#### Comment

The second element addresses the scienter requirement for the crime of computer fraud. The language differs in one important aspect from the language in the credit card fraud statute, where a defendant must have acted "knowingly and with intent to defraud."<sup>2</sup> In contrast, the first three subsections of 18 U.S.C. § 1030(a) require the defendant to commit the acts specified in the indictment merely "knowingly" or "intentionally."

The jury is instructed as to the definition of "knowingly." "Knowingly" is given its meaning in the language of the Model Penal Code, namely, acting voluntarily and deliberately, rather than by accident. The "knowing" state of mind in section 1030(a) parallels that in 18 U.S.C. § 1029(a), the credit card fraud statute.<sup>3</sup> In its legislative history, Congress referred to Model Penal Code § 2.02(7) and stated that it intended a "knowing" state of mind to mean "(1) an awareness of the nature of one's conduct, and (2) an awareness of the nature of or a firm belief in the existence of a relevant circumstance such as whether [the device is a computer]."<sup>4</sup>

The jury is also charged that the scienter element may be satisfied by proof of deliberate disregard for whether the defendant has actual knowledge of the

<sup>2</sup> 18 U.S.C. § 1029(a).

<sup>3</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 20 (1984).

<sup>4</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 16 (1984).

accessing of a computer either without authority or outside the scope of authority. This instruction is consistent with the congressional intent that a "knowing" state of mind could be satisfied by proof that the defendant "was aware of a high probability of the existence of the circumstance."<sup>5</sup> Instruction 40A-5 properly balances the "awareness of the high probability" standard with the "unless the defendant actually believed" counterpoint, as prescribed by *United States v. Cano*.<sup>6</sup>

A successful defense, however, may rest upon proof that the defendant "actually believed that the circumstance did not exist after taking reasonable steps to warrant such belief."<sup>7</sup> In Congress' view, "willful blindness" exists only when the defendant is aware of a high probability of the existence of a relevant circumstance "but does not satisfy himself that it does not in fact exist."<sup>8</sup> Thus, a defendant is held responsible for negating his own suspicions of illegality; by not doing so, he will be considered to have acted with the requisite knowledge. Nonetheless, care must be taken not to shift the burden of proof to the defendant on this issue. Thus, Instruction 40A-5 properly imposes the burden on the government to satisfy this element beyond a reasonable doubt.<sup>9</sup>

<sup>5</sup> *United States v. Morris*, 928 F.2d 504 (2d Cir.), *cert. denied*, 502 U.S. 817 (1991).

<sup>6</sup> 702 F.2d 370 (2d Cir. 1983). *See also* *United States v. Kallash*, 785 F.2d 26 (2d Cir. 1986).

<sup>7</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 20 (1984).

<sup>8</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 17 (1984), *quoting* *United States v. Jewell*, 532 F.2d 697, 700 n.7 (9th Cir.), *cert. denied*, 426 U.S. 951 (1976).

<sup>9</sup> *United States v. Kallash*, 785 F.2d 26 (2d Cir. 1986).

## Instruction 40A-6

## Third Element—Obtaining of Protected or Restricted Information

The third element that the government must prove beyond a reasonable doubt is that the defendant obtained information protected against unauthorized disclosure for reasons of national defense or foreign relations or any restricted data, with the intent to use such information against the interests of the United States.

The United States may determine that information requires protection against unauthorized disclosure for reasons of national defense or foreign relations either by Executive Order or by statute.

"Restricted data" is defined as all data concerning (1) the design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy.

This element requires that at the time he obtained the protected or restricted information, the defendant must have had reason to believe that the information could be used against the interests of the United States or to the advantage of a foreign nation.

---

Authority

18 U.S.C. § 1030(a)(1).

42 U.S.C. § 2014(y).

H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 21 (1984).

---

Comment

In the legislative history, Congress noted the substantial federal interest in protecting against the unauthorized access of highly sensitive material.<sup>1</sup> Restricted data does not include data declassified or removed from the restricted data category pursuant to 42 U.S.C. § 2162.<sup>2</sup>

<sup>1</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 20 (1984).

<sup>2</sup> 42 U.S.C. § 2014(y).

Congress intended the definition of classified information to parallel that of the federal espionage laws.<sup>3</sup> According to *Gorin v. United States*,<sup>4</sup> to act "with the intent or reason to believe" that the classified information is to be used against the interests of the United States requires that the defendant acted with bad faith.<sup>5</sup>

This element was substantially altered by the amendments contained in the Economic Espionage Act of 1996.<sup>6</sup> Prior to the 1996 amendments, this element contained a substantial mens REA element: that the defendant intended to use the information to the detriment of the United States or to the advantage of a foreign nation. The 1996 Act eliminated the scienter requirement with respect to this element, but incorporated a new willfulness element with respect to the communication of the information to another person.<sup>7</sup>

This subsection of the Act contains neither a monetary threshold amount nor a requirement that the access affects interstate or foreign commerce, although earlier versions of the Act contained such provisions.<sup>8</sup>

<sup>3</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 20 (1984). See 18 U.S.C. § 793.

<sup>4</sup> 312 U.S. 19, 61 S. Ct. 429, 85 L. Ed. 488 (1940).

<sup>5</sup> 312 U.S. at 28. See also *United States v. Trong Dinh Hung*, 629 F.2d 908, 918-19 (4th Cir. 1980); *United States v. Smith*, 592 F. Supp. 424, 429-30 (E.D. Va. 1984).

<sup>6</sup> Pub. L. No. 104-294, § 201(1)(A)(iv), 110 Stat. 3501 (1996).

<sup>7</sup> See Instruction 40-7, *below*. See also Instruction 3A-3, *above*.

<sup>8</sup> H.R. Rep. No. 98-894, 98th Cong., 2d Sess. 20 (1984).

## Instruction 40A-7

## Fourth Element—Willful Communication of Improperly Obtained Information

The fourth element that the government must prove beyond a reasonable doubt is that the defendant willfully communicated (*or delivered or transmitted or caused to be communicated, delivered, or transmitted or attempted to communicate, deliver, transmit*) the protected or restricted information obtained to any person not entitled to receive it (*or willfully retained that information and failed to deliver it to the officer or employee of the United States entitled to receive it*).

To act willfully means to act knowingly and purposely, with an intent to do something the law forbids, that is to say, with a bad purpose either to disobey or disregard the law. There is no requirement that the defendant acted for financial gain. (*If applicable: While proof of financial gain may be considered by you as evidence of the defendant's bad purpose, it is not necessary that the government prove such financial gain in order to satisfy this element.*)

---

Authority

18 U.S.C. § 1030(a)(1)

---

Comment

The fourth element was added by the Economic Espionage Act of 1996.<sup>1</sup>

<sup>1</sup> Pub. L. No. 104-294, § 201(1)(A)(vi), 110 Stat. 3501 (1996).

## UNITED STATES

V.

**MANNING, Bradley E., PFC**

U.S. Army,

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**DEFENSE REPLY TO  
GOVERNMENT  
SUPPLEMENTAL RESPONSE  
TO DEFENSE MOTION TO  
COMPEL DISCOVERY #2**

DATED: 11 July 2012

1. The Defense requests that this Court order the Government to disclose discovery from the State Department in accordance with R.C.M. 701(a)(2), 701(a)(6) and 703, as discussed herein. Further, the Defense requests that this Court deny the Government's request for 45-60 days to produce relevant records or claim a privilege or move for substitutions. Instead, the Defense requests that this Court order that for all remaining discovery, the Government should consult with equity holders to coordinate the claiming of a privilege (or other course of action) *simultaneous* with its review of the documentation such that the Government is prepared to proceed immediately upon a discovery ruling.

**A. The Government Fails To Indicate Whether Any of the State Department Records Contained *Brady* Material**

2. The Government's submission overlooks a critical issue: Do any of the State Department records contain *Brady* material? Now that it has reviewed all these records, it is in a position to state whether the records contained *Brady*. Nowhere in its submission does it say whether it found *Brady* material. Instead, it says "absent that which is discoverable under Brady or RCM 701(a)(6), information that predated, and contributed to, the Department's draft damage assessment is cumulative, and thus not subject to production under RCM 703." Prosecution Supplemental Response to Defense Motion to Compel Discovery #2, at p. 4 [hereinafter "Government Response"]. First thing's first. Do any of the records reveal *Brady* material? If so, these records need to be immediately disclosed to the Defense. Moreover, based on the tenor of the Government's submissions, the Defense would like to be clear: information can be discoverable *Brady* material even if it is cumulative.

3. The Defense is not clear why the Government failed to overlook this critical issue in its submission. However, it would venture to guess that some material which it describes as

"predating" the State Department damage assessment actually constitutes *Brady* material. Thus, the Defense believes that the Government is hoping that if the Court rules that anything predating the damage assessment does not need to be produced, it will get out of its *Brady* obligations that way.

**B. The Court Should Deny the Government's Request to Not Produce Records that Predate the State Department Damage Assessment**

4. The Government wants this Court to rule that *anything* that predated the State Department damage assessment should not be produced because it is cumulative and not relevant and necessary. It states in this respect:

The following categories contain information that predated, and likely contributed to, the Department's draft damage assessment, and therefore are cumulative:

- (1) Written assessments produced by the Chiefs of Mission used to formulate a portion of the draft damage assessment completed in August of 2011;
- (2) Written Situational Reports produced by the WikiLeaks Working Group between roughly 28 November 2010 and 17 December 2010;
- (3) Written minutes and agendas of meetings by the Mitigation Team;
- (4) Information Memorandum for the Secretary of State produced by WPAR;
- (5) Matrices produced by WPAR to track identified individuals; and
- (6) Formal guidance produced by WPAR and provided to all embassies, including authorized actions for any identified person at risk.

The Government is asking for permission to simply exclude from discovery anything with a date that preceded the State Department damage assessment – which would, in effect, be *practically everything at the State Department*. It would have the Court do so on the sheer conjecture that this information "likely contributed to[] the Department's draft damage assessment." Government Response, at p. 5.

5. The Government's request is breathtaking. It would have the Court deny discovery of facially relevant information because this information was "likely" considered by the State Department in compiling the damage assessment. The Government does not even bother to try to make the argument that the discovery is *actually* cumulative (i.e. it is duplicative of information in the damage assessment). That argument would not be true. Instead, it makes the argument that based on the fact that this material predates the damage assessment, it *must be* cumulative (i.e. it is *de facto* cumulative). The Government's lack of logic continues to dumbfound the Defense.

6. Consider the implications of this request. All an agency would need to do to avoid discovery is to compile some type of ultimate assessment and then claim that anything that predated that



assessment was "off limits" because it was somehow "considered" in developing the assessment. The contention is ludicrous.

7. Further, the volume of information that the Government would seek to have the court exclude from its discovery obligations is in the ballpark of 5000 pages. The Government believes that these 5000 pages must have "likely contributed to" the 150 page State Department damage assessment.<sup>1</sup> It is hard to believe that the damage assessment is cumulative when, page-wise, there are thirty-three times more pages in the disputed discovery than in the damage assessment itself.

8. The State Department's "interim" damage assessment is not the be-all-and-end-all of discovery from the State Department in this case. If there are other documents dealing with mitigation efforts, the damage from the charged cables, etc., this is all evidence that is material to the preparation of the defense under R.C.M. 701(a)(2), and thus, relevant and necessary under R.C.M. 703. It does not matter whether it predated the damage assessment or was considered by those drafting the damage assessment.

9. Let's look at a couple of the categories of information that the Government would have the Court rule "off-limits" because they temporally predate the State Department damage assessment. The Government would seek to preclude the Defense from having access in discovery to the "Formal guidance produced by WPAR and provided to all embassies, including authorized actions for any identified person at risk." Because this predated the damage assessment, according to the Government, it is overcome by events. However, the formal guidance provides insight into the degree of remediation that was necessary and the true seriousness of the alleged leaks. If the guidance, for instance, indicated that major remediation measures needed to be taken, this is something that would clearly be material to the preparation of the defense (i.e. the Defense would then know not to argue that this did not cause much disruption at the State Department). It would also be information that would not be discoverable under *Brady*. Thus, if this Court accepts the Government's request, this evidence would never see the light of day simply because it predated the damage assessment.

10. The Government would also seek to prevent the Defense from having access to the written assessments by the Chiefs of Mission review. Assume, for instance, that the Ambassador from Country A indicated that the leaks did little to no damage in his country. Assume further that the State Department damage assessment downplays this fact and does not accurately portray the actual assessment by the Ambassador from Country A. How is this information not material to the preparation of the defense (or relevant and necessary) simply because it predated the damage assessment? The Defense would clearly want to know if the State Department damage assessment overstated the damage, or potential for damage, from the alleged leaks.

11. Much like the testimony of the Original Classification Authorities (OCAs), the Government would have the Defense and Court treat the "interim" State Department damage assessment as absolute gospel that cannot be questioned. It would have everyone pretend that nothing that happened before the creation of the damage assessment was important or relevant.

---

<sup>1</sup> This is the Defense's estimate based on only reviewing the damage assessment on one occasion. The Defense does not have its own copy of the damage assessment.

12. The Government's request to have this Court order outright exclusion of all discovery that predates the State Department damage assessment is particularly egregious in light of the Government listing *twenty-two* witnesses from the State Department. How can the Government in good faith plan on calling twenty-two witnesses from the State Department and refuse to turn over documentation on the sole basis that because it predates the damage assessment, it is "likely" cumulative? See Government Response, p. 5 ("The following categories contain information that predated, and likely contributed to, the Department's draft damage assessment, and therefore are cumulative."). This would certainly make it easier for the Government to prepare their witnesses. After all, the Defense would be limited in its cross examination to basically one document – the damage assessment – which the Defense does not have the ability to even view absent coordination with the Government.

13. And the Defense need not remind the Court that, to the extent that the Defense does use the damage assessment against the Government and its State Department witnesses, we already know that the Government is planning on arguing that the assessment is only "interim" – or, in the words of the Government, it represents "a snapshot in time." Thus, the Government plans on downplaying the significance of the document that now contends is the *only* document that the Defense should have from the State Department. How can the Government be permitted to talk out of both sides of its mouth – say that the damage assessment is only "interim" and therefore not particularly significant, but that it is significant enough that all other information that predates it should not be produced to the Defense?

14. What is funny is if the Government was planning on going this ridiculous route, why did it even need to review the documentation? It knew on 7 June (over one month ago) that virtually all the information specifically listed by the Defense predated the damage assessment. The only information that did not predate the damage assessment is the information collected by the Director of the Office of Counter Intelligence and Consular Support. So why wait a month to make this argument? Nothing in this argument actually relies on the content of the documents the Government has reviewed. Instead, it simply relies on the dates at the top of the document. Given this, the argument could have been presented (and disposed of) much earlier.

15. The Government's argument that anything that predates the draft damage assessment is not discoverable is so weak that it is reminiscent of the *Giles* argument. This Court will recall that the Government insisted that the State Department damage assessment was not discoverable based on dicta in a second concurring opinion from a 50-year old case. The Government acknowledged that its argument was made at the behest of the State Department; when the Defense questioned the Government on this, it adopted the position as its own. Here, the Government has once again adopted a litigation position that is so untenable that it should be embarrassing. One is left to wonder the obvious question: Is the Government actually making these arguments of its own accord, or is the State Department the puppet master in this case? The Defense would venture to guess that it is the latter. If so, this is clearly a conflict of interest; a third party government agency cannot be permitted to dictate the litigation positions of the prosecutor in a criminal proceeding. The agency's role is limited to claiming a privilege if discovery is ordered by a Court. An agency cannot be "in cahoots" with the Government to formulate trial strategy that would be best for that agency. As the Defense has said before, the Government's litigation positions are always borne of convenience and not of principle. This is yet another example of the Government taking a preposterous litigation position in order to

champion the interests of the State Department – the organization that will provide, incidentally, nearly a quarter of the witnesses in this case.

**C. The Court Should Deny the Government's Request to Not Produce "Purely Administrative" Records**

16. The Government requests that the Court relieve it from the obligation to provide "purely administrative records without any substantive value or that have no identifiable connection with the relevant mitigation effort." Government Response, at p. 5. The Defense does not understand the second part of the sentence ("without any substantive value or that have no identifiable connection with the relevant mitigation effort"), and how that sentence is intended to modify the scope of "purely administrative records." Normally, the Defense would trust that the Government could distinguish between a pure administrative record and something else. Unfortunately, that is not so in this case. Given the liberties that the Government has taken with all definitions in this case, the Defense does not understand what the Government means by "purely administrative records" – much less what it means by "purely administrative records without any substantive value or that have no identifiable connection with the relevant mitigation effort." *Id.*

17. Moreover, even purely administrative records might be material to the preparation of the defense. If there is, for instance, a log book that chronicles how many times a group met and for how long, that can be used to show the extent of the concern that the disclosure of the cables caused at the State Department. While this is just one example, the Defense simply does not believe that the Government will distinguish between administrative and non-administrative records in good faith.

**D. The Court Should Deny the Government's Request to Not Produce Information About Persons at Risk**

18. The Government makes a beyond-feeble attempt to resist production of information related to persons at risk:

PII of persons negatively affected by the accused's charged misconduct, particularly those persons put at risk based on the released Department cables, is not discoverable under Brady or RCM 701(a)(6). Further, such information is not relevant and necessary under RCM 703 because such information, *inter alia*, would not "contribute to a party's presentation of the case in some positive way on a matter in issue." Even if material to the preparation of the defense, any PII of persons put at risk based on the released Department cables is not material to the preparation of the defense to the extent that it is relevant and necessary.

Government Response, at p. 6. While the Government does a good job of parroting back discovery rules, it fails to explain *why* the information is not material to the preparation of the defense or relevant and necessary. It seems somewhat obvious to the Defense that if the Government is going to show, either in the merits or sentencing, that the disclosures put certain people at risk, then the Defense is entitled to information pertaining to those people apparently put at risk. If the Government wishes to claim a privilege over this information, it is entitled to

do so. However, it appears highly disingenuous to claim that this information is not material to the preparation of the defense.

19. If the Government refuses to produce this information to the Defense, the Defense will move to preclude the Government from making any reference in this case to the release of the diplomatic cables putting people at risk. The Government wants to have its cake and eat it too. It wants to call twenty-two witnesses from the State Department who will opinion on how catastrophic the leaks were and how they put innocent lives at risk – all while refusing to provide underlying documentation regarding those individuals apparently put at risk. The Defense submits that this is the equivalent of entering a boxing ring with your hands tied behind your back. How can the Defense attempt to rebut any allegation that these individuals were not put at risk without any underlying documentation?

**E. The Government's Contention that a Written Statement of Ambassador Kennedy's Testimony Does Not Exist is Not Believable**

20. The Government states:

The Department did not find any prepared written statements for the Department's reporting to Congress on 7 and 9 December 2010. Based on those dates and Under Secretary Kennedy's testimony, only informal discussions would have occurred between Department officials and members of Congress, therefore there are no written statements or other documents.

Government Response, at p. 4. The Defense submits that it is likely that neither the Government nor the State Department tried hard enough.

21. Notably, the Government does not state definitively that no written statement exists. Rather it states, "[b]ased on those dates and Under Secretary Kennedy's testimony, only informal discussions would have occurred between Department officials and members of Congress, therefore there are no written statements or other documents." *Id.* So it appears to be sheer conjecture that no such statement exists. Indeed, it defies logic that Ambassador Kennedy would appear before Congress and simply "wing it." Moreover, why would Ambassador Kennedy have a written statement on 10 March 2011 for the Senate Committee on Homeland and Governmental Affairs, but not for his reporting to Congress?

22. Neither the Government nor the State Department has an incentive to look very hard for any written statement that Ambassador Kennedy made to Congress. In the end, we are left with the million dollar question is: *Did anybody ask Ambassador Kennedy?*

**F. The Defense Requests That the Court Order the Government to Be Prepared to Claim (or Not Claim) a Privilege Immediately Upon a Discovery Ruling**

23. Perhaps the most troubling aspect of the Government's motion is its request on p. 6:

Assuming, *arguendo*, the Court orders production of the above records or some portion thereof, the prosecution requests no less than 45-60 days to notify the Court whether the Department will seek limited disclosure under MRE 505(g)(2)

or claim a privilege under MRE 505(c) and to produce the documents under RCM 701(g), MRE 505(g)(2), or MRE 505(c), if necessary.

This is the Government's not-so-subtle attempt to hold the Court and the Defense hostage to its timeline. This simply cannot continue.

24. This case has been ongoing for 26 months (approximately 800 days). The Government would seek to add on time to the case calendar as if it were nothing. Let it forget, PFC Manning is still in pretrial confinement. And the only reason why the parties are currently still in the "discovery phase" of litigation (as stated by MAJ Fein in his letter to the General Counsel of ONCIX) is because the Government has been grossly negligent in fulfilling its discovery obligations.

25. Consider for a moment what the Government's request means in practical terms. The Government filed this motion on 9 July 2012. The Defense's Response will be filed on 11 July 2012. The issue will likely be litigated at the next motions argument on 16-20 July -- assuming the Government does not file a motion opposing the Defense's request to have the Court deny the Government an additional 45-60 days. If the Court rules on, say, 20 July 2012 that the evidence is discoverable, the Government would then have until 20 September to "seek limited disclosure under MRE 505(g)(2) or claim a privilege under MRE 505(c) and to produce the documents under RCM 701(g), MRE 505(g)(2), or MRE 505(c), if necessary." Litigation would then ensue over the limited disclosure or privilege, which would bring the parties to November or December.

26. The Defense cannot fathom why the Government cannot multi-task -- i.e. why can't the Government review the documents and simultaneously consult with the equity holder about what documents would be subject to a claim of privilege or limited disclosure? If the Government would simply apply some common sense, it would be in a position (even under its timeline) to proceed within the next few weeks.

27. The Government will undoubtedly say that the Defense simply does not understand how complicated this process is, etc. We have heard this all before. At some point, the Government cannot continue to hide behind the complexity of this case as an excuse for everything. It has the entire resources of the United States government behind it -- including the ability to contract out work to lawyers who are not even detailed to this case (which the Defense is aware that the Government is currently doing). The Government cannot continue to requests months upon months to produce discovery that should have, in fact, been produced *well over a year ago*.

28. The Defense would also like this Court to take note of the difficult position that the Government has put the Court in -- a position that the Defense submits was designed to manipulate the Court into ruling in the Government's favor. If the Court rules in the Defense's favor and orders the Government to produce some or all of the records, it will not be until likely November or December that this issue is settled. It might be that, after reviewing these records, the Defense becomes aware of other discovery that should have been produced. After all, the purpose of discovery is to "discover" information. Thus, we may be well into the New Year and still mired in discovery battles regarding the State Department. The one sure-fire way to avoid all this would be to rule in the Government's favor -- a quick and easy fix. The Defense is

clearly not saying that the Court will be persuaded by the Government's tactics; it is simply saying that it was the deliberate intention of the Government to lord discovery delays over the Court and the Defense in hopes of avoiding its discovery obligations.

29. The Defense incorporated dates for disclosure of State Department documents into its case calendar because it knew that the Government would seek to drag out the process as long as conceivably possible. The Government resisted putting any such dates on its calendar, saying instead, "No disclosure is scheduled for DoS documents because the motion has not been litigated. The DoS Discovery litigation is scheduled for the 16-20 July 2012 session." 30 June 2012 Email from MAJ Fein to the Court. The Government's position is typical in that it adopts the most protracted, nonsensical way of doing things. Rather than planning ahead in order to expedite the discovery process, the Government proceeds as if things simply cannot, or should not, be done simultaneously. Given how long has elapsed since PFC Manning has been placed in pretrial confinement, the Government's cavalier attitude in constantly requesting "at a minimum, an additional 45-60 days" is disquieting.

**G. The Defense Requests That The Government Be Required to Provide All Documentation it has Received from the State Department**

30. The Government simply cannot be trusted to make decisions regarding discovery in this case. This latest motion shows that the Government believes that anything that predates an interim damage assessment is *de facto* cumulative and therefore not discoverable. If the Government is prepared to make such an inane argument, it is clear that the Government simply cannot be trusted to sift through what is *Brady* and what is material to the preparation to the defense and/or relevant and necessary.

31. At a certain point, the Government should have to "own" its litigation positions. It cannot continue to make arguments that are so far out in left field that they raise questions about the basic ability of the Government to recognize what is material to the preparation of the defense and/or what is relevant and necessary. A blanket exclusion of all discovery based on an arbitrary date (the date of the State Department damage assessment) is not an intelligent, reasonable litigation position. And when prosecutors continue to take widely unreasonable litigation positions, at a certain point, they can no longer be trusted.

32. As a reminder, here are but a few of the highly untenable legal positions the Government has taken in this case, just with respect to discovery:

- a) Maintaining that *Brady* did not apply to punishment;
- b) Maintaining that R.C.M. 701 did not apply to classified discovery;
- c) Disputing the relevance of facially relevant items (such as damage assessments);
- d) Maintaining that R.C.M. 703 applied to discovery, instead of the appropriate R.C.M. 701 standard;
- e) Resisting production of the Department of State damage assessment under the "authority" of *Giles* (which provided no legal support for its position);
- f) Debating with the Court on whether the Government needed to provide documents that were obviously material to the preparation of the defense absent a specific request;

- g) Maintaining that the FBI investigative file was not material to the preparation of the defense, to which the Court quizzically asked, "How could the investigative file *not* be material to the preparation of the defense?"
- h) Maintaining that the Defense did not provide the requisite level of specificity (e.g. for files that could not conceivably have been described any more specifically)

33. The Defense understands that whether certain things are discoverable may be the subject of litigation. However, the Government has taken such extreme and unsupported positions over the course of this litigation that the Defense and the Court are left to wonder whether: a) the Government has any idea what it is doing; and b) in light of past events, the Government can be trusted to do what the Court orders.

34. Accordingly, the Defense submits that the only way to ensure that the Defense gets the discovery it is entitled to is for the Court to order that all documentation from the State Department be produced to the Defense. Alternatively, the Government should be required to segregate all discovery that it does *not* believe needs to be produced and order that the Government be required to produce it to the Court for *in camera* review.

#### CONCLUSION

35. For the reasons outlined herein, the Defense requests that this Court deny the Government's request to not be required to produce the following information:

- (1) Information that predated the State Department draft damage assessment dated August 2011;
- (2) Purely administrative records; and
- (3) Personally Identifiable Information (PII) of persons negatively affected by the unauthorized disclosures, to include those persons identified by the WikiLeaks Persons at Risk Group (WPARG) as being put at risk.

36. The Defense renews its motion for production of information from the State Department in accordance with R.C.M. 701(a)(2), 701(a)(6) and 703, as discussed herein. Further, the Defense requests that this Court deny the Government's request for 45-60 days to produce relevant records or claim a privilege or move for substitutions. Instead, the Defense moves for this Court to order that for all remaining discovery, the Government should consult with equity holders to coordinate the claiming of a privilege (or other course of action) *simultaneous* with its review of the documentation such that the Government is prepared to proceed immediately upon a discovery ruling.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE REPLY TO  
GOVERNMENT RESPONSE TO  
DEFENSE REQUESTED  
INSTRUCTION:  
SPECIFICATION 1 OF CHARGE  
II**

DATED: 11 July 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 920(c), requests this Court to give the instructions requested in the Defense Requested Instruction: Specification 1 of Charge II [hereinafter Defense Requested Instruction].

ARGUMENT

2. Each of the Government's responses to the Defense Requested Instructions is meritless. They are discussed in turn.

**A. Wantonly**

3. The Government first takes issue with the Defense's proposed definition of "wantonly." The Defense Requested Instruction defines "wantonly" as follows: "'Wanton' or 'wantonly' includes 'Reckless' but may connote willfulness, or a disregard of probable consequences, and thus describe a more aggravated offense." Defense Requested Instruction, at 2. This definition of wantonly is taken nearly verbatim from the only two places in the entire Manual for Courts-Martial (MCM) where that term is defined.

4. The MCM does not define the term "wanton" in the context of disclosure of information, but it does define the term in two other contexts. See MCM, Part IV, para. 35.c(8) (defining "wanton" for purposes of Article 111); *id.*, Part IV, para. 100a.c(4) (defining "wanton" for purposes of Article 134, offense of "reckless endangerment"). Both definitions provided by the MCM are essentially the same: "'Wanton' includes 'Reckless' but may connote willfulness, or a disregard of probable consequences, and thus describe a more aggravated offense." *Id.*, Part IV, para. 100a.c(4); see *id.*, Part IV, para. 35.c(8) ("Wanton" includes 'reckless', but in describing the operation or physical control of a vehicle, vessel, or aircraft 'wanton' may, in a proper case, connote willfulness, or a disregard of probable consequences, and thus describe a more aggravated offense.').



5. In its Response, the Government states merely that it “maintains that ‘wantonly’ does not necessarily describe a more aggravated offense than ‘recklessness.’” Government Response to Defense Motion for Requested Instruction: Specification 1 of Charge II [hereinafter Government Response], at 1. For one thing, the Government misunderstands the definition of “wantonly” provided by the Defense. That definition does not state that “wantonly” necessarily describes a more aggravated offense than recklessness. It merely states that wantonly “*may* connote willfulness, or a disregard of probable consequences, and thus describe a more aggravated offense [than recklessness].” Defense Requested Instruction, at 2 (emphasis supplied). For another thing, the Government offers no reason for disregarding authoritative definitions of wantonly provided in the MCM. In its own proposed instruction for “wantonly,” the Government cites the Military Judges Benchbook, DA Pam 27-9 [hereinafter Benchbook], paragraph 3-35-1, n. 10. The Government conveniently omits from its proposed instruction the following line contained in the definition of “wantonly” provided by this Benchbook paragraph: “Wantonness also includes willful conduct.” Benchbook, para. 3-35-1, n. 10. Thus, the Government’s own source supports the definition proposed by the Defense, and undermines the Government’s definition. Therefore, this Court should adopt the Defense’s proposed definition of “wantonly.”

**B. Caused to be Published**

6. The Government also objects to the Defense’s proposed instruction to the “caused to be published” element. The Defense Requested Instruction proposed the following instruction for “caused to be published:”

A person causes intelligence to be published on the Internet when the person personally publishes the intelligence on the Internet or knowingly or intentionally induces or sets in motion acts by an animate or inanimate agency or instrumentality which result in the publication of the intelligence on the Internet.

Defense Requested Instruction, at 2.

7. The Government complains that “[t]his instruction will confuse the fact finder. There is no requirement that the act be carried out ‘knowingly or intentionally.’ The act must be done wrongfully and wantonly.” Government Response, at 1. The Government is incorrect. The Government has itself necessitated an instruction on “cause to be published” by including this language in Specification 1 of Charge II. *See* Charge Sheet. Moreover, the Government alleged that PFC Manning caused this intelligence to be published on the Internet having knowledge that information published on the Internet is accessible to the enemy. *See id.* The Defense Requested Instruction has defined the phrase “caused to be published” for the court-martial members. The Government, in its proposed instructions, failed to define this phrase. The Government cannot charge a particular phrase in the Specification and then simply invite the Court to refrain from defining that phrase for the members.

**C. Maximum Punishment**

8. Finally, the Government objects to the Defense’s characterization of this offense as being most closely related to a violation of Article 92. Identifying a single additional element that Specification 1 of Charge II contains that a violation of Article 92 does not, the Government

concludes, with no analysis of how this additional element compels its conclusion, that "[t]he offense is more closely-related to a violation of 18 U.S.C. § 793(e)." Government Response, at 1. This cursory argument stands in stark contrast to the argument made in the Defense Requested Instruction.

9. The Defense identified three reasons why a violation of Article 92 is the offense most closely related to the offense alleged in Specification 1 of Charge II. *See* Defense Requested Instruction, at 3 ("First, Specification 1 of Charge II and a violation of AR 380-5 have similar mens rea requirements: the charged specification requires that an accused act wrongfully and wantonly (including recklessness, willfulness, or a disregard of probable consequences), and AR 380-5 punishes one who 'knowingly, willfully, or negligently' discloses covered information, AR 380-5, para. 1-21(a). Second, the intelligence information covered by Specification 1 of Charge II is likely within the definitions of 'classified information' or 'sensitive information' contained in AR 380-5. Finally, the conduct underlying the offense alleged in the charged specification is closely related to the conduct that would constitute a violation of AR 380-5: the disclosure of information to an unauthorized person or entity."). In addition to not providing any thought out reasons to support its own conclusory assertions, the Government has offered no rebuttal to any of the three reasons offered by the Defense.

10. Therefore, a violation of Article 92 is the offense that is most closely related to the offense alleged in Specification 1 of Charge II, and the maximum punishment for both offenses is two years imprisonment.

#### CONCLUSION

11. For these reasons, the Defense requests this Court to give the instructions requested in the Defense Requested Instruction.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel



505(h)(3) prior to the Article 32 investigation, but identified the witness it intended to discuss the information with during the hearing. *See* Enclosure.

### WITNESSES/EVIDENCE

The United States requests this Court consider the Enclosure and Appellate Exhibit XXXII in support of its motion.

### LEGAL AUTHORITY AND ARGUMENT

Under MRE 505(h)(1), if the accused reasonably expects to disclose or to cause the disclosure of classified information in any manner in connection with a court-martial proceeding, he must provide notice to the trial counsel in writing of his intention. MRE 505(h)(1). This notice must include a brief description of the classified information and "must state, with particularity, which items of classified information [the accused] reasonably expects will be revealed by his defense." MRE 505(h)(3). A general statement "of the areas about which evidence may be introduced" is not sufficient. *Id.* The accused's notice under MRE 505(h) allows the Government to consider the relevance of the classified information and, if required, motion the court for an *in camera* proceeding concerning the use at any proceeding of the classified information identified by the accused. *See* MRE 505(i)(2). In order to obtain an *in camera* proceeding, the Government must be able to demonstrate that disclosure of the information reasonably could be expected to cause damage to the national security. MRE 505(i)(3). This showing is typically achieved through a classification review of the information identified by the defense notice to the Government. *See* MRE 505(i)(3) ("The affidavit shall demonstrate that disclosure of the information reasonably could be expected to cause damage to the national security in the degree required to warrant classification under the applicable executive order, statute, or regulation."). Classified information is not subject to disclosure unless the information is relevant and necessary to an element of the offense or a legally cognizable defense and is otherwise admissible in evidence. MRE 505(i)(4)(B).

#### I. PORTIONS OF THE DEFENSE NOTICE UNDER MRE 505(h)(3) DO NOT PROVIDE ENOUGH SPECIFICITY TO THE GOVERNMENT.

The United States objects to the notice provided in paragraphs 2a, 2b, 2e<sup>1</sup>, and 2h; specifically, the portion of each paragraph providing notice in the following terms: "The Defense also intends to discuss, in general, the [records] that are the subject of [Specification X] of Charge II." *See* Def. Not. at 1-4. Those portions provide insufficient notice of the classified information the accused intends to disclose or cause the disclosure of under both the plain language of MRE 505(h) and *United States v. Collins*, 720 F.2d 1195 (11th Cir. 1983)<sup>2</sup>.

---

<sup>1</sup> The United States has the same objection to paragraph 2e, although the defense notice is articulated somewhat differently.

<sup>2</sup> Subsection (h)(3) was amended in 1993 to require specificity in detailing the items of classified information expected to be introduced, based on the *Collins* case. *See* MRE 505 analysis, at A22-41.

Written notice under MRE 505(h) is the “central document” in MRE 505. *See Collins*, 720 F.2d at 1199 (discussing MRE 505’s counterpart in the Classified Information Procedures Act). The notice must be sufficient because it is “essential to put into motion the other [MRE 505] procedures.” *Id.* at 1198. In this case, the defense has stated it “intends to discuss, in general” the documents or records that are the subject of Specifications 4, 6, 8, and 12 of Charge II. Although this is indeed a “brief” description of the information or material at issue, it is the functional equivalent of referring the United States to the Charge Sheet. “Brief” does not mean notice to the United States may be “vague.” *See id.* at 1199. The notice in this case does not state, with any sort of particularity, which items of classified information the accused intends to reveal in his defense. *See* MRE 505(h)(3). These databases, in total, contain hundreds of thousands of documents or records. *See* Def. Not. at 1-4; Charge Sheet. Each document or record is marked differently. The notice provided by the defense is inadequate because it fails to provide the United States with a starting point. In this case, the starting point could be a unique report key for CIDNE records or a unique message record number for Department of State cables.<sup>3</sup> In any event, if it is unclear as to which specific items of classified information are at issue, the United States cannot make a determination whether to concede the relevance, necessity, or admissibility of the information or, in the alternative, request a classification review from the relevant OCA and move the court for an *in camera* proceeding under MRE 505(i). If the *in camera* proceeding under MRE 505(i) is where all roads lead under MRE 505, the defense’s lack of particularity drops the United States in the middle of a forest with no hope of finding home.

Adequate notice drives the procedures under MRE 505. It focuses the issues for the parties and the Court and contributes to the efficiency of the proceedings. Without adequate notice, the United States is left to guess what the accused means by the notice provided and delays the Government’s decision whether to invoke the privilege. That uncertainty delays the classification review process, which in turn delays the ability of the United States to motion the Court to hold an *in camera* proceeding under MRE 505(i). Most importantly, adequate notice contributes to this Court’s timely resolution of the issues prior to trial.

## II. THE DEFENSE NOTICE IS ALSO INADEQUATE BECAUSE IT DOES NOT IDENTIFY WITNESSES.

The United States also objects to the notice provided in paragraphs 2a-2j because it does not identify the names of any witnesses it intends to discuss classified information with during trial. Prior to the Article 32 investigation, the defense provided notice under MRE 505(h)(3) of its intent to disclose classified information during the hearing. *See* Enclosure. In that notice, the defense specifically identified the witness it intended to discuss classified information with during the hearing. *Id.* The Court signed the Protective Order for Classified Information on 16 March 2012. *See* Appellate Exhibit XXXII. Under paragraph 3(l), the defense is required “to provide the trial counsel with the names of any intended recipient(s) and notice of the classified


---

<sup>3</sup> The United States has only conducted a classification review for the charged documents identified by Bates Number. The vast majority of the other records referred to by the defense were provided on digital media in classified discovery because they originated from classified databases. Their classification has not been determined by a competent authority.

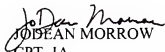
information that is expected to be disclosed or elicited pursuant to MRE 505(h)(3).” Appellate Exhibit XXXII, at 6. The defense has acknowledged this requirement in writing and should be required, at this time, to identify the Government witnesses it intends to elicit classified information from during trial to promote judicial economy and efficiency.<sup>4</sup> Further, without knowing the witnesses the defense intends to use to disclose classified information during trial, the United States is not fully able to contemplate what other classified information may be revealed by cross-examination, which could potentially vary by witness.

### CONCLUSION

The United States respectfully requests this Court order the defense to supplement its Notice Under MRE 505(h)(3) with respect to paragraphs 2a, 2b, 2e, and 2h by identifying, with particularity, the items of classified information the defense intends to reveal during trial. Additionally, the United States requests the Court order the defense to supplement its notice by identifying the witness or witnesses the defense intends to use to elicit classified information.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 11 July 2012.

  
JODEAN MORROW  
CPT, JA  
Assistant Trial Counsel

Encl  
Article 32 Notice

---

<sup>4</sup> The United States acknowledges the defense has likely not finalized its own witness list and therefore would be unable to provide adequate notice with respect to defense witnesses at this time.

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE NOTICE UNDER  
MILITARY RULE OF EVIDENCE**

**505(h)(3)**

DATED 22 November 2011

1. Pursuant to Military Rule of Evidence 505(h)(3), PFC Manning, by and through counsel, provides notice to the government that the defense intends to present, either through cross-examination of the government's witnesses or during the defense's presentation, the following evidence during the Article 32 hearing:

a. CIDNE Afghanistan Significant Activity Reports (SIGACTs). The CIDNE Afghanistan SIGACTs consist of 91,731 documents covering a period from 1 January 2004 to 31 December 2009. The defense intends to discuss each individual SIGACT report that is the subject of Specification 7 of Charge II with Vice Admiral Robert S. Harward. Specifically, the defense intends to discuss Vice Admiral Harward's classification determination and his determination regarding the impact on national security from having this information released publicly. The defense also intends to discuss, in general, the Afghanistan SIGACT reports that are the subject of Specification 6 of Charge II with Vice Admiral Harward;

b. CIDNE Iraq SIGACTs. The CIDNE Iraq SIGACTs consist of 391,832 documents covering a period from 1 January 2004 to 31 December 2009. Again, the defense intends to discuss each individual SIGACT report that is the subject of Specification 5 of Charge II with Vice Admiral Robert S. Harward. Specifically, the defense intends to discuss Vice Admiral Harward's classification determination and his determination regarding the impact on national security from having this information released publicly. The defense also intends to discuss, in general, the Iraq SIGACT reports that are the subject of Specification 4 of Charge II with Vice Admiral Harward;

c. Other Briefings as well as the Granai Airstrike Video and accompanying 15-6 Investigation Report. This information contains a video of an airstrike that took place on 4 May 2009 along with the resulting 15-6 investigation and numerous other briefings. The airstrike involved the dropping of 500lb and 1,000lb bombs on a suspected militant compound. The bombing resulted in anywhere between 80 to 140 civilians being killed. The defense intends to discuss each individual item listed on page 14 and 15 of Vice Admiral Harward's classification review. Some of this information also appears to be the subject of Rear Admiral Kevin M. Donegan's classification review. Specifically, the defense intends to discuss Vice Admiral

Harward's and Rear Admiral Donegan's classification determinations and their determination regarding the impact on national security from having this information released publicly. The items referenced are the subject of Specifications 10 and 11 of Charge II;

d. A diplomatic cable known as Reykjavik-13. This diplomatic cable was from the embassy in Reykjavik detailing the financial difficulties of a privately owned Icelandic bank called Landsbanki, which offered online savings accounts under the "Icesave" brand. The bank was placed into receivership by the Icelandic Financial Supervisory Authority on 7 October 2008. The defense intends to discuss the diplomatic cable that is the subject of Specification 14 of Charge II with Mr. Patrick F. Kennedy. Specifically, the defense intends to discuss Mr. Kennedy's classification determination and his determination regarding the impact on national security from having this information released publicly;

e. Diplomatic cable database. This database contains 251,287 documents. The contents of the cables describe international affairs from 300 embassies dating from 1966 to 2010. Over 130,000 of the documents are unclassified, some 100,000 are labeled "confidential", about 15,000 documents are classified as "secret", and none are classified as "top secret." The defense intends to discuss each diplomatic cable that is the subject of Specification 13 of Charge II with Mr. Patrick F. Kennedy. Specifically, the defense intends to discuss Mr. Kennedy's classification determination and his determination regarding the impact on national security from having this information released publicly. The defense also intends to discuss the diplomatic cables in general that are the subject of Specification 12 of Charge II with Mr. Kennedy;

f. Apache Helicopter Video. A thirty-nine minute Apache cockpit gun-sight video depicting a series of air-to-ground attacks conducted by a team of two U.S. Army AH-64 Apache helicopters in Al-Amin al-Thaniyah, in the district of New Baghdad in Baghdad. The attacks took place on 12 July 2007. In the first strike, 30mm cannon fire was directed at a group of nine men; two were war correspondents for Reuters Saeed Chmagh and Namir Noor-Elden. Eight men were killed, including Noor-Eldeen. Chmagh was wounded. In the second airstrike, 30mm cannon fire was directed at Chmagh and two other unarmed men and their unmarked van as they were attempting to help Chmagh into the van. Two children inside the van were wounded, three more men were killed, including Chmagh. In a third airstrike, an Apache helicopter team fired three AGM-114 Hellfire missiles to destroy a building after they had observed men enter the building. The defense intends to discuss the Apache helicopter video that is the subject of Specification 2 of Charge II with CPT James Kolky. Specifically, the defense intends to discuss CPT Kolky's classification determination and his determination regarding the impact on national security from having this information released publicly;

g. U.S. Army's Threat Assessment. A thirty-two page document prepared by the Cyber Counterintelligence Assessments Branch of the Army's Counterintelligence Center along with the National Ground Intelligence Center to assess the counterintelligence threat posed to the U.S. Army by Wikileaks. This document is the subject of Specification 15 of Charge II. The defense intends to discuss the threat assessment with the individual who is identified as completing the classification review. Specifically, the defense intends to discuss the classification determination and the determination regarding the impact on national security from having this information released publicly;

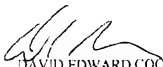


h. The Guantanamo Files. This database consists of 779 Secret case files. These memoranda contain information about each prisoner to include their background; how they were captured; whether they are regarded as low; medium or high risk; whether they should be released or not. The defense intends to discuss each document that is the subject of Specification 9 of Charge II with Rear Admiral David Woods. Specifically, the defense intends to discuss the classification determination of Rear Admiral Woods and the determination regarding the impact on national security from having this information released publicly. The defense also intends to discuss, in general, the Guantanamo files that are the subject of Specification 8 of Charge II;

i. Government Intelligence Agency Memorandums. Specification 3 of Charge II alleges that between 22 March 2010 and 26 March 2010 PFC Manning unlawfully disclosed "more than one classified memorandum produced by a United States government intelligence agency." The defense intends to discuss each document that is the subject of Specification 3 of Charge II with Mr. Robert L. Roland. Specifically, the defense intends to discuss Mr. Roland's classification determination and his determination regarding the impact on national security from having this information released publicly.

j. Chat Log. A text log of a computer chat session allegedly between Mr. Adrian Lamo and PFC Manning. Although the log has no classification markings, according to Mr. Robert E. Betz, it contains national security information properly classified at the SECRET level. The defense intends on exploring the subject matter of the text log with Mr. Betz. Specifically, the defense intends to discuss Mr. Betz's classification determination and his determination regarding the impact on national security from having this information released publicly.

2. Nothing contained in this notice should be construed in any manner as a concession by PFC Manning or his defense that the listed items are appropriately classified pursuant to Executive Order 13256 or that the disclosure of such information would be detrimental to the national security.

  
DAVID EDWARD COOMBS  
Civilian Defense Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Prosecution Response

to Defense Proposed  
Court Member Questionnaire

11 July 2012

1. The prosecution recommends that the Court adopt the prosecution's Proposed Court Member Supplemental Questionnaire (hereinafter "Supplemental Questionnaire"). See Enclosure 2. The Supplemental Questionnaire includes the questions asked by the defense and the prosecution that elicit information relevant to a member's participation in this case or information that could be used to inform the exercise of challenges or expedite voir dire. The Supplemental Questionnaire excludes the questions that are cumulative, confusing, misstatements of law, or impermissibly attempt to convey factual material to the court members to argue the defense's case.

2. The purpose of the court member questionnaires is to provide counsel with general information relevant to a member's participation in a particular case. Rules of Practice Before Army Courts-Martial, dated 26 March 2012 (hereinafter "Rules of Practice"), Appendix E, p.25. Using questionnaires can also expedite voir dire and be used to permit more informed exercise of challenges. Rule for Courts-Martial (RCM) 912(a)(1), Discussion; Rules of Practice, Rule 13.1, p.8.

3. Voir Dire exists so parties can intelligently exercise both challenges for cause and peremptory challenges. See RCM 912(d), Discussion ("The opportunity for voir dire should be used to obtain information for the intelligent exercise of challenges."); United States v. Bragg, 66 M.J. 325, 327 (C.A.A.F. 2008) ("The purpose of voir dire and challenges is, in part, to ferret out facts, to make conclusions about the members' sincerity, and to adjudicate the members' ability to sit as part of a fair and impartial panel."). Voir dire should not purposely be used "to present factual matters which will not be admissible or to argue the case." RCM 912(d), Discussion; see, e.g., United States v. Nieto, 66 M.J. 146 (C.A.A.F. 2008) (discussing the difference between appropriate hypothetical questions and commitment improper commitment questions); United States v. Reynolds, 23 M.J. 292, 294 (C.M.A. 1987) ("Neither the Government nor the accused is entitled to a commitment from the triers of fact about what they will ultimately do."); United States v. Smith, 2007 WL 3025072 (N-M. Ct. Crim. App.) (finding defense excluded questions "misstated the law, were confusing, cumulative, or appeared principally crafted to convey factual material to the members rather than to elicit information upon which to base challenges"); United States v. Moran, 1999 WL 219759 (A.F. Ct. Crim. App.) (calling defense counsel's "objectionable question . . . a poorly veiled attempt to argue for no punitive discharge"). Similarly, questionnaires should not purposely be used to present factual matters which will not be admissible or to argue the case as such questions neither assist in providing counsel with relevant information about the members nor assists in voir dire and the informed exercise of challenges. See United States v. Anderson, 36 M.J. 963 (A.F.C.M.R. 1993), aff'd, 39 M.J. 431 (C.M.A. 1994) ("When the inquiry seeks more than the public has a right to know, the matter lies within the judge's discretion . . .").

4. RCM 912(f) enumerates the bases for challenges for cause. RCM 912(f)(1)(A)-(M) spell out bases for removal for cause. RCM 912(f)(1)(N) states that a court member shall be excused for cause when the removal is "in the interest of having the court-martial free from substantial doubt as to legality, fairness, and impartiality." RCM 912(f)(1)(N). For example, an individual has a direct personal interest in the result of the trial; has a friendly or hostile attitude toward a party; or has an inelastic opinion concerning an appropriate sentence for the offenses charged. RCM 912(f)(1)(N), Discussion. Case law has defined two separate tests to define what types of opinions may cause substantial doubt as to legality, fairness, and impartiality--actual and implied bias. Actual bias is bias that, viewed subjectively, through the eyes of the military judge, "will not yield to the evidence presented and the judge's instructions." United States v. Napoleon, 46 M.J. 279, 283 (C.A.A.F.1997) (quoting Reynolds, 23 M.J. at 294). Implied bias is viewed objectively, through the eyes of the public, and "exists when 'most people in the same position would be prejudiced.'" United States v. Daulton, 45 M.J. 212, 217 (C.A.A.F. 1996) (quoting United States v. Smart, 21 M.J. 15, 20 (C.M.A.1985)); see United States v. Strand, 59 M.J. 455, 459 (C.A.A.F. 2004) ("In making judgments regarding implied bias, this Court looks at the totality of the factual circumstances.")

5. RCM 912(g) addresses peremptory challenges and gives examples of reasons for which peremptory challenges are not allowed. See RCM 912(g), Discussion.

6. IAW RCM 912(a)(1), upon application of the defense, the prosecution shall ask the following information of court members in written questionnaires: date of birth; sex; race; marital status and sex, age, and number of dependents; home of record; civilian and military education, including, when available, major areas of study, name of school or institution, years of education, and degrees received; current unit to which assigned; past duty assignments; awards and decorations received; date of rank; and whether the member has acted as accuser, counsel, investigating officer, convening authority, or legal officer or staff judge advocate for the convening authority in the case, or has forwarded the charges with a recommendation as to disposition. RCM 912(a)(1). Additional questions may be asked with the approval of the military judge. Id.

7. Panel members on the standing MDW panel have completed the standard MDW Court Member Questionnaire (hereinafter "MDW Questionnaire"). See Enclosure 1. Several of the questions requested by the defense were already asked on the MDW Questionnaire; however, not all defense requested questions were included. The attached Supplemental Questionnaire, therefore, includes the nonobjectionable defense questions that were not previously answered by panel members, as well as additional prosecution requested questions. See Enclosure 2. Some of the included defense requested questions were rephrased for consistency, clarity, and/or to include more or less information.

a. The following is the prosecution's response to the defense questionnaire by corresponding question number:

- 1) The prosecution included this question on the Supplemental Questionnaire.

2) Panel members already answered the question regarding their place and date of birth on the MDW Questionnaire. The prosecution included the questions regarding the sex and race of court members on the Supplemental Questionnaire.

3) The prosecution included this question on the Supplemental Questionnaire.

4) Panel members already answered the question regarding their current duty station and phone number on the MDW Questionnaire; however, the prosecution included an updated request in the Supplemental Questionnaire to ensure the parties have the most current information.

5) Panel members already answered these questions on the MDW Questionnaire; however, the prosecution included an updated request in the Supplemental Questionnaire to ensure the parties have the most current information.

6) Panel members already answered the question regarding MOS and job title on the MDW Questionnaire. The prosecution included the questions regarding description of job, length of present assignment and name and title of supervisor on the Supplemental Questionnaire.

7) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire. Every Soldier will answer yes to the first part of the question, and reviewing the court members' ORBs/ERBs will be more instructive on the court member's leadership experience than a yes or no question. The second part of the question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask this question, therefore, is to impermissibly convey factual material to the court members to argue the defense's case.

8-9) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask these questions, therefore, is to impermissibly convey factual material to the court members to argue the defense's case.

10-11) The prosecution included these questions on the Supplemental Questionnaire.

12-13) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask these questions, therefore, is to impermissibly convey factual material to the court members to argue the defense's case.

14) Panel members already answered this question on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.

15) The prosecution objects to this question because it is confusing. The prosecution is not sure what the defense means by combat. If the defense means deployments, panel members deployments are listed on their ERBs/ORBs.

16) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask this question is to impermissibly convey factual material to the court members to argue the defense's case.

17-18) Panel members already answered these questions on the MDW Questionnaire.

19) Panel members already answered this question on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.

20) The prosecution included this question on the Supplemental Questionnaire, but has restricted the question from "have you ever" to the last 10 years. This is in line with the questionnaire in the Rules of Practice which limits the past duty assignment inquiry to the past 10 years.

21-22) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire.

23) The prosecution included this question on the Supplemental Questionnaire.

24-28) Panel members already generally answered these questions on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.

29) Panel members already generally answered this question on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.

30-31) The prosecution consolidated these questions and included the question on the Supplemental Questionnaire.

32) Panel members already generally answered this question on the MDW Questionnaire and have the opportunity to elaborate their answer in the question asked based on defense requested 30-31. Any additional inquiry can be explored during individual voir dire.

33) The prosecution included this question on the Supplemental Questionnaire.

34) Panel members already generally answered this question on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.

35) The prosecution objects to this question because it is confusing. The prosecution is not sure what the defense means by combat. In the event that the defense is asking about deployments, the prosecution included this question on the Supplemental Questionnaire.

- 36) The prosecution included this question on the Supplemental Questionnaire.
- 37-39) The prosecution consolidated these questions and included the questions on the Supplemental Questionnaire.
- 40) Panel members already generally answered this question on the MDW Questionnaire and have the opportunity to elaborate their answer in the question asked based on defense requested 39. Any additional inquiry can be explored during individual voir dire.
- 41) Panel members already generally answered this question on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.
- 42-43) The prosecution consolidated these questions and included a question on the Supplemental Questionnaire. Any additional inquiry can be explored during individual voir dire.
- 44) Panel members already generally answered this question on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.
- 45) The prosecution included this question on the Supplemental Questionnaire.
- 46) Panel members already generally answered this question on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.
- 47) The prosecution objects to this question because it is confusing. The prosecution is not sure what the defense means by combat. In the event that the defense is asking about deployments, the prosecution included this question on the Supplemental Questionnaire.
- 48-54) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire.
- 55) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask this question is to impermissibly convey factual material to the court members to argue the defense's case.
- 56-57) The prosecution included these questions on the Supplemental Questionnaire.
- 58) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask this question is to impermissibly convey factual material to the court members to argue the defense's case.
- 59) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire.

60) The prosecution included this question on the Supplemental Questionnaire.

61-62) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire.

63-66) The prosecution included these questions on the Supplemental Questionnaire.

67-69) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire.

70) The prosecution included this question on the Supplemental Questionnaire.

71-74) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire.

75) Panel members already answered this question on the MDW Questionnaire.

76-82) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask this question is to impermissibly convey factual material to the court members to argue the defense's case.

83) The prosecution included this question on the Supplemental Questionnaire.

84-85) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire.

86) The prosecution included these questions on the Supplemental Questionnaire.

87-88) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire.

89-91) Panel members already generally answered this question on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.

92) The prosecution included this question on the Supplemental Questionnaire.

93) Panel members already generally answered this question on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.

94) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire.

95) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire. Defense requested question #92 and any additional voir dire will reveal sufficient information to determine if the court member has any biases towards the mental health profession.

96) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire.

97-100) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire. There is no credible evidence that the Accused suffered from abuse.

101-102) The prosecution included these questions on the Supplemental Questionnaire.

103) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire.

104-105) The prosecution included these questions on the Supplemental Questionnaire.

106) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask this question is to impermissibly convey factual material to the court members to argue the defense's case.

107-109) Panel members already generally answered these questions on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire.

110) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire.

111-115) Panel members already generally answered these questions on the MDW Questionnaire. Any additional inquiry can be explored during individual voir dire

116) The prosecution included this question on the Supplemental Questionnaire.

117-118) The prosecution included these questions on the Supplemental Questionnaire.

119) The prosecution objects to the introductory statements in this question. The prosecution, therefore, made the statements more neutral and less communicative of the facts of the case, and still included the defense requested question on the Supplemental Questionnaire.



120-121) The prosecution included these questions on the Supplemental Questionnaire.

122) The prosecution included these questions on the Supplemental Questionnaire.

123) This question includes a misstatement of law. UCMJ action could never be initiated based on sexual preference.

124-130) The prosecution included these questions on the Supplemental Questionnaire.

131) This question elicits no information relevant to a member's participation in this case, nor elicits information that could be used to inform exercise of challenges or expedite voir dire.

Gender Identity Disorder paragraph. The prosecution objects to defense's definition of gender identity disorder as the alleged disorder is irrelevant to this case. The only reason to discuss the alleged disorder is to impermissibly convey factual material to the court members to argue the defense's case.

132-134) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask this question is to impermissibly argue the defense's case.

135) The prosecution included this question on the Supplemental Questionnaire.

136-137) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask this question is to impermissibly argue the defense's case.

138) Panel members deployments are listed on their ERBs/ORBs.

139-140) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire. The only reason to ask this question is to impermissibly argue the defense's case.

141) The prosecution made this defense requested question broader and included the question on the Supplemental Questionnaire.

Punishment paragraph. The prosecution objects to defense's punishment description. The military judge defines the law and instructions for the court members, not the defense.

142) The prosecution included this question on the Supplemental Questionnaire.

143) The prosecution changed the objectionable wording of the question ("noble . . . goal") and included this defense requested question on the Supplemental Questionnaire.

144) The prosecution included this question on the Supplemental Questionnaire.

145) The prosecution changed the objectionable wording of the question ("who has given classified information to an unauthorized person") and included this defense requested question on the Supplemental Questionnaire.

146) The prosecution included this question on the Supplemental Questionnaire.

147) See #145 above. This is the same question.

148) The prosecution included this question on the Supplemental Questionnaire.

149) These questions elicit no information relevant to a member's participation in this case, nor elicit information that could be used to inform exercise of challenges or expedite voir dire.

150) The prosecution included this question on the Supplemental Questionnaire.

151) The prosecution included this question on the Supplemental Questionnaire.

b. The prosecution recommends adding the following questions which elicit information relevant to a member's participation in this case without impermissibly conveying factual material or arguing the prosecution's case:

1) Have you ever had a SIPRNET account or worked on a classified computer?

2) Have you ever handled classified information in any form?

3) Have you ever printed classified information or saved classified information to a CD or other removable media?

4) Have you ever worked in a Sensitive Compartmented Information Facility (SCIF)?

5) Have you ever worked in a facility that authorized open storage of classified information?

6) Have you ever removed classified information from a government facility?

7) Have you ever been an authorized courier of classified information?

8. The prosecution recommends the Court adopt the prosecution's proposed questionnaire, which accounts for the questionnaires already completed by all panel members, incorporates the questions requested by the defense which are relevant and permissible, and incorporates the questions requested by the prosecution which elicit information that will assist in voir dire without conveying impermissible argument or factual material.



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Defense Counsel via electronic mail, on 11 July 2012.



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

2 Enclosures

1. MDW Standard Questionnaire
2. Prosecution Proposed Additional Questions

$\mathbf{y}_i$ 

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**Enclosure 1**

**11 July 2012**

DATA REQUIRED BY THE PRIVACY ACT OF 1974

AUTHORITY: THE COMMON LAW AND RCM 923, MANUAL FOR COURTS-MARTIAL, 2005 (HEREAFTER REFERRED TO AS MCM).

PURPOSE: INFORMATION PROVIDED IS USED BY THE TRIAL COUNSEL AND DEFENSE COUNSEL TO PREPARE FOR THE VOIR DIRE EXAMINATION OF COURT MEMBERS.

ROUTINE USES: THE INFORMATION PROVIDED BY THE COURT MEMBER IN THIS QUESTIONNAIRE WILL BE ONLY USED BY THE TRIAL COUNSEL, THE DEFENSE COUNSEL, AND THEIR ASSISTANTS, AND IN SOME CASES, BY THE STAFF JUDGE ADVOCATE AND THE CONVENING AUTHORITY, TO SELECT FAIR AND IMPARTIAL COURT MEMBERS FOR COURTS-MARTIAL. COUNSEL WILL USE THE INFORMATION PROVIDED IN THE PREPARATION OF QUESTIONS TO BE USED DURING THE VOIR DIRE EXAMINATION OF COURT MEMBERS. COUNSEL MAY ALSO USE INFORMATION PROVIDED IN THESE QUESTIONNAIRES AND THE RESULTING ANSWERS GIVEN IN OPEN COURT TO CHALLENGE COURT MEMBERS FOR CAUSE UNDER THE PROVISIONS OF PARAGRAPH 912 (F), MCM. THE INFORMATION PROVIDED WILL NOT BE RELEASED TO OTHER THAN THE CONVENING AUTHORITY, THE STAFF JUDGE ADVOCATE, COUNSEL, AND THEIR ASSISTANTS. NOTE, HOWEVER, THAT ANY INFORMATION PROVIDED BY A COURT MEMBER IN OPEN COURT IS A MATTER OF PUBLIC RECORD.

COMPLETION OF THE QUESTIONNAIRE IS VOLUNTARY AND YOU MAY ELECT NOT TO ANSWER CERTAIN QUESTIONS YOU DEEM ARE TOO PERSONAL. HOWEVER, IF THE QUESTIONNAIRE IS NOT COMPLETED, COUNSEL AT A COURT-MARTIAL MAY SEEK THE SAME INFORMATION DURING THE VOIR DIRE EXAMINATION.

**COURT MEMBER QUESTIONNAIRE**  
**(PLEASE PRINT CLEARLY)**

1. NAME: \_\_\_\_\_ SSN: \_\_\_\_\_
2. RANK: \_\_\_\_\_ DATE OF RANK: \_\_\_\_\_
3. UNIT ASSIGNMENT: \_\_\_\_\_
4. PRESENT DUTY POSITION: \_\_\_\_\_
5. (FOR OFFICERS ONLY)
  - A. PRIMARY SPECIALTY: \_\_\_\_\_
  - B. SECONDARY SPECIALTY: \_\_\_\_\_
  - C. SOURCE OF COMMISSION: \_\_\_\_\_
  - D. HAVE YOU HAD ANY ENLISTED SERVICE? \_\_\_\_ YES \_\_\_\_ NO
6. (FOR ENLISTED ONLY) MOS/JOB TITLE: \_\_\_\_\_
7. BRANCH OF SERVICE: \_\_\_\_\_
8. HAVE YOU SERVED IN ANOTHER ARMED FORCES OR BRANCH OF SERVICE?  
\_\_\_\_ YES \_\_\_\_ NO (IF YES, PLEASE INDICATE):  
\_\_\_\_\_  
\_\_\_\_\_
9. YEARS OF ACTIVE DUTY: \_\_\_\_\_
10. DATE OF BIRTH: \_\_\_\_\_ PLACE OF BIRTH: \_\_\_\_\_
11. HOME OF RECORD: \_\_\_\_\_
12. MARITAL STATUS: \_\_\_\_\_
13. AGE AND SEX OF CHILDREN (E.G., 12, MALE):  
\_\_\_\_\_  
\_\_\_\_\_

**COURT MEMBER QUESTIONNAIRE (CONTINUED)**

14. WHAT, IF ANY, IS YOUR RELIGIOUS PREFERENCE? \_\_\_\_\_

15. TOTAL YEARS OF CIVILIAN EDUCATION: \_\_\_\_\_

A. ARE YOU A HIGH SCHOOL GRADUATE? \_\_\_\_ YES \_\_\_\_ NO

B. HAVE YOU ATTENDED COLLEGE (UNDERGRADUATE)? \_\_\_\_ YES \_\_\_\_ NO  
(IF YES, INDICATE THE FOLLOWING):

1ST COLLEGE

2D COLLEGE

NAME OF COLLEGE: \_\_\_\_\_

YEARS OF ATTENDANCE: \_\_\_\_\_

FIELD OF STUDY: \_\_\_\_\_

MINOR FIELD(S): \_\_\_\_\_

DEGREE(S) AWARDED: \_\_\_\_\_

C. HAVE YOU ATTENDED GRADUATE SCHOOL? \_\_\_\_ YES \_\_\_\_ NO  
(IF YES, INDICATE THE FOLLOWING):

1ST UNIVERSITY

2D UNIVERSITY

NAME OF UNIVERSITY: \_\_\_\_\_

YEARS OF ATTENDANCE: \_\_\_\_\_

FIELD OF STUDY: \_\_\_\_\_

DEGREE AWARDED: \_\_\_\_\_

16. HAVE YOU ATTENDED LAW SCHOOL OR TAKEN ANY LAW COURSES? (INCLUDE MILITARY SCHOOLS): \_\_\_\_ YES \_\_\_\_ NO

SCHOOL

DATE

COURSE/TOPIC

A. \_\_\_\_\_

B. \_\_\_\_\_

C. \_\_\_\_\_

COURT MEMBER QUESTIONNAIRE (CONTINUED)

17. SUMMARY OF MILITARY EDUCATION COMPLETED:

<u>NAME OF SCHOOL</u>	<u>COURSE</u>	<u>YEAR COMPLETED</u>
-----------------------	---------------	-----------------------

A. \_\_\_\_\_

B. \_\_\_\_\_

C. \_\_\_\_\_

D. \_\_\_\_\_

E. \_\_\_\_\_

(CONTINUE ON LAST PAGE IF NECESSARY).

18. SUMMARY OF MILITARY CAREER (LAST TEN YEARS, PLUS ANY SIGNIFICANT OR UNUSUAL ASSIGNMENTS):

<u>FROM/TO</u>	<u>COMMAND</u>	<u>DUTY ASSIGNMENT</u>
----------------	----------------	------------------------

A. \_\_\_\_\_

B. \_\_\_\_\_

C. \_\_\_\_\_

D. \_\_\_\_\_

E. \_\_\_\_\_

F. \_\_\_\_\_

G. \_\_\_\_\_

H. \_\_\_\_\_

I. \_\_\_\_\_

J. \_\_\_\_\_

(CONTINUE ON LAST PAGE IF NECESSARY).



**COURT MEMBER QUESTIONNAIRE (CONTINUED)**

19. HAVE YOU OR ANY CLOSE RELATIVES OR CLOSE FRIENDS EVER BEEN INVOLVED IN ANY OF THE FOLLOWING AREAS? \_\_\_\_ YES \_\_\_\_ NO (IF YES, CHECK APPLICABLE AREA AND EXPLAIN BRIEFLY).

\_\_\_\_ CRIME PREVENTION (POLICE, SHERIFF, DETECTIVE, ETC.)

\_\_\_\_ MEDICINE (DOCTOR, NURSE, PHARMACIST, ETC.)

\_\_\_\_ MENTAL HEALTH (PSYCHIATRIST, PSYCHOLOGIST, ETC.)

\_\_\_\_ LAW (JUDGE, ATTORNEY, LAW STUDENT, ETC.)

\_\_\_\_ CAREER MILITARY (CLOSE RELATIVES ONLY)

A. \_\_\_\_\_

B. \_\_\_\_\_

C. \_\_\_\_\_

(CONTINUE ON LAST PAGE IF NECESSARY).

20. HAVE YOU EVER SERVED AS A LEGAL OFFICER? \_\_\_\_ YES \_\_\_\_ NO  
(IF YES, INDICATE THE FOLLOWING):

DATE

COMMAND

DESCRIPTION OF DUTIES

A. \_\_\_\_\_

B. \_\_\_\_\_

21. HAVE YOU (AS OIC/COMMANDING OFFICER) EVER CONVENED:

NUMBER      YEAR(S)

A. SUMMARY COURTS-MARTIAL:

\_\_\_\_ YES \_\_\_\_ NO

\_\_\_\_\_

B. SPECIAL COURTS-MARTIAL:

\_\_\_\_ YES \_\_\_\_ NO

\_\_\_\_\_

C. ARTICLE 32 INVESTIGATIONS:

\_\_\_\_ YES \_\_\_\_ NO

\_\_\_\_\_

D. HAVE YOU EVER IMPOSED NONJUDICIAL PUNISHMENT UNDER ARTICLE 15?

\_\_\_\_ YES \_\_\_\_ NO

**COURT MEMBER QUESTIONNAIRE (CONTINUED)**

22. HAVE YOU EVER SERVED AS A SUMMARY COURT-MARTIAL OFFICER?

\_\_\_\_ YES \_\_\_\_ NO (IF YES, INDICATE THE FOLLOWING):

NUMBER OF TIMES: \_\_\_\_\_ DATES (YEARS ONLY): \_\_\_\_\_

23. HAVE YOU EVER SERVED AS A TRIAL COUNSEL OR DEFENSE COUNSEL?

\_\_\_\_ YES \_\_\_\_ NO (IF YES, INDICATE THE FOLLOWING):

NUMBER OF TIMES: \_\_\_\_\_ DATES (YEARS ONLY): \_\_\_\_\_

24. HAVE YOU BEEN APPOINTED AS A MEMBER OF A GENERAL OR SPECIAL COURT-MARTIAL WITHIN THE LAST 12 MONTHS? \_\_\_\_ YES \_\_\_\_ NO (IF YES, INDICATE THE FOLLOWING):

CASE NAME

MO/YR

SPCM

GCM

A. \_\_\_\_\_

B. \_\_\_\_\_

C. \_\_\_\_\_

25. HAVE YOU HAD EXPERIENCE AS A MEMBER OF A GENERAL OR SPECIAL COURT-MARTIAL PRIOR TO THE LAST 12 MONTHS? \_\_\_\_ YES \_\_\_\_ NO  
(IF YES, PLEASE INDICATE THE FOLLOWING):

HOW MANY TIMES

DATE (YEARS ONLY)

SPCM: \_\_\_\_\_

GCM: \_\_\_\_\_

26. HAVE YOU, OR ANY CLOSE RELATIVE, EVER BEEN A VICTIM OF A CRIME? (DO NOT INCLUDE MINOR INCIDENTS): \_\_\_\_ YES \_\_\_\_ NO (IF YES, INDICATE NATURE OF THE CRIME, HOW LONG AGO IT OCCURRED, THE RELATIONSHIP OF THE VICTIM TO YOU, WHETHER THE PERPETRATOR WAS ARRESTED OR CONVICTED).

A. \_\_\_\_\_

B. \_\_\_\_\_

C. \_\_\_\_\_

(CONTINUE ON LAST PAGE IF NECESSARY).

**COURT MEMBER QUESTIONNAIRE (CONTINUED)**

27. HAVE YOU EVER SERVED AS A JUROR IN A CIVILIAN TRIAL (EITHER STATE OR FEDERAL)?  
\_\_\_\_ YES \_\_\_\_ NO (IF YES, INDICATE AS FOLLOWS):

YEAR   CIVIL OR CRIMINAL CASE

STATE OR FEDERAL COURT

- A. \_\_\_\_\_  
B. \_\_\_\_\_  
C. \_\_\_\_\_

28. HAVE YOU EVER BEEN A WITNESS AT A COURT-MARTIAL? \_\_\_\_ YES \_\_\_\_ NO

29. IS THERE ANYTHING IN YOUR BACKGROUND OR EXPERIENCE THAT MIGHT AFFECT YOUR  
ABILITY TO SERVE AS A MEMBER OF THE COURT? \_\_\_\_ YES \_\_\_\_ NO  
(IF YES, EXPLAIN BRIEFLY).

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

30. PLEASE PROVIDE THE FOLLOWING INFORMATION TO ENSURE THAT WE ARE ABLE TO  
CONTACT YOU:

- A. DUTY PHONE: \_\_\_\_\_  
B. HOME PHONE: \_\_\_\_\_  
C. CELLUAR PHONE: \_\_\_\_\_  
D. PAGER: \_\_\_\_\_  
E. E-MAIL ADDRESS: \_\_\_\_\_  
F. DUTY FAX: \_\_\_\_\_  
F. DUTY MAILING  
ADDRESS \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

) ) ) ) ) ) ) ) )

**Y.**

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**Enclosure 2**

**11 July 2012**

**COURT MEMBER**  
**SUPPLEMENTAL QUESTIONNAIRE**  
(PLEASE PRINT CLEARLY)

This questionnaire is submitted to detailed court members under Rule for Courts-Martial 912(a)(1), Manual for Courts-Martial. Its purpose is to provide counsel with general information relevant to a member's participation in a particular case. This information will be made available to trial and defense counsel before trial so that they may have general information about a member's background before assembly of the court and is also available to the military judge. Disclosure of this information is voluntary. Nondisclosure may require a member to provide such matters at trial. By requesting this information on a one-time basis before you actually serve as a member, repetitive questions and unnecessary delay can be avoided. Your responses should be forwarded to the Office of the Staff Judge Advocate, ATTN: Chief, Criminal Law Division.

1. Name: \_\_\_\_\_
2. Rank: \_\_\_\_\_ 3. Date of rank: \_\_\_\_\_
4. Sex: \_\_\_\_\_ 5. Race: \_\_\_\_\_
6. Unit Assignment: \_\_\_\_\_
7. Present Duty Position and Description: \_\_\_\_\_
8. Length of Present Assignment: \_\_\_\_\_
9. Name and Title of Supervisor: \_\_\_\_\_
10. Summary of residences for past three years:

FROM/TO

CITY, STATE, COUNTRY

- A. \_\_\_\_\_
- B. \_\_\_\_\_
- C. \_\_\_\_\_
- D. \_\_\_\_\_

(Continue on last page if necessary)

11. Have you ever had a SIPRNET account or worked on a classified computer? \_\_\_\_ YES \_\_\_\_ NO
12. Have you ever handled classified information in any form? \_\_\_\_ YES \_\_\_\_ NO

13. Have you ever printed classified information or saved classified information to a CD or other removable media? \_\_\_\_ YES \_\_\_\_ NO

14. Have you ever worked in a Sensitive Compartmented Information Facility (SCIF)? \_\_\_\_ YES \_\_\_\_ NO

15. Have you ever worked in a facility that authorized open storage of classified information?  
\_\_\_\_ YES \_\_\_\_ NO

16. Have you ever removed classified information from a government facility? \_\_\_\_ YES \_\_\_\_ NO

17. Have you ever been an authorized courier of classified information? \_\_\_\_ YES \_\_\_\_ NO

18. Have you ever been denied a security clearance or had a security clearance revoked? \_\_\_\_ YES \_\_\_\_ NO  
If yes, please indicate when and the reason: \_\_\_\_\_

19. Are you aware of Soldiers who have been denied security clearances or had security clearances revoked?  
\_\_\_\_ YES \_\_\_\_ NO If yes, please indicate when, the reason, and your involvement (if any): \_\_\_\_\_

---

20. Summary of civilian employment for past ten years (if any):

<u>FROM/TO</u>	<u>EMPLOYER</u>	<u>TITLE/DUTIES</u>
----------------	-----------------	---------------------

A. \_\_\_\_\_

B. \_\_\_\_\_

C. \_\_\_\_\_

D. \_\_\_\_\_

(Continue on last page if necessary)

21. Do you have any difficulty reading or writing the English language? \_\_\_\_ YES \_\_\_\_ NO If yes, please explain: \_\_\_\_\_

22. Do you have any dependants besides your children and spouse (listed on original questionnaire)?  
\_\_\_\_ YES \_\_\_\_ NO If yes, please list their relationship to you, as well as their sex and age: \_\_\_\_\_

---

23. Summary of current and/or former spouse's employment for past ten years (if any):

<u>FROM/TO</u>	<u>EMPLOYER</u>	<u>TITLE/DUTIES</u>
----------------	-----------------	---------------------

A. \_\_\_\_\_

B. \_\_\_\_\_

C. \_\_\_\_\_

D. \_\_\_\_\_

E. \_\_\_\_\_

F. \_\_\_\_\_

G. \_\_\_\_\_

(Continue on last page if necessary)

24. What special recognitions, awards, medals, or commendations did your current and/or former spouse receive (if any)? \_\_\_\_\_

25. Has your current and/or former spouse deployed? \_\_\_\_ YES \_\_\_\_ NO If yes, please give dates and locations: \_\_\_\_\_

26. Is your current and/or former spouse a high school graduate? \_\_\_\_ YES \_\_\_\_ NO

27. Has your current and/or former spouse attended any technical or trade schools or college, as an undergraduate or graduate student? \_\_\_\_ YES \_\_\_\_ NO If yes, indicate the following:

1ST SCHOOL

2D SCHOOL

3D SCHOOL

Name of school: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Location: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Years Attended: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Major: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Minor: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Degree(s)

Received (if any): \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

28. Has your current and/or former spouse attended any military training/education? \_\_\_\_ YES \_\_\_\_ NO  
If yes, indicate the following:

NAME OF SCHOOL COURSE/AREA OF STUDY YEARS ATTENDED DEGREES AWARDED

A. \_\_\_\_\_

B. \_\_\_\_\_

C. \_\_\_\_\_

D. \_\_\_\_\_

E. \_\_\_\_\_

(Continue on last page if necessary)

29. How many individuals lived in the household in which you were raised? \_\_\_\_\_ What was their relationship to you (e.g., father, stepbrother, etc.)? \_\_\_\_\_

30. Did any family member receive any special recognitions, awards, medals, or commendations for serving in any branch of the Army Forces? \_\_\_\_\_ YES \_\_\_\_\_ NO If yes, please list them: \_\_\_\_\_

31. Have any of your family members deployed? \_\_\_\_\_ YES \_\_\_\_\_ NO If yes, please give dates and locations: \_\_\_\_\_

32. What newspapers do you regularly read or subscribe to (if any)? \_\_\_\_\_

33. What magazines, journals, or other periodicals do you regularly read or subscribe to (if any)? \_\_\_\_\_

34. How often do you listen to the radio? \_\_\_\_\_ To which stations and/or programs do you listen? \_\_\_\_\_

35. What is your main source of news? \_\_\_\_\_

36. Which television news programs do you watch? \_\_\_\_\_

37. Are you most interested in local, state, national, or world news? \_\_\_\_\_

38. Do you typically watch any news magazine programs (Dateline NBC, 20/20, 60 Minutes, 48 Hours, etc.)? \_\_\_\_\_ YES \_\_\_\_\_ NO If yes, which programs? \_\_\_\_\_

39. How would you describe yourself on social issues (e.g., very conservative, conservative, moderate, liberal, very liberal) and why? \_\_\_\_\_



40. How would you describe yourself on religious issues (e.g., very conservative, conservative, moderate, liberal, very liberal) and why? \_\_\_\_\_

41. How would you describe yourself on political issues (e.g., very conservative, conservative, moderate, liberal, very liberal) and why? \_\_\_\_\_

42. What is your general opinion about psychiatrists, psychologists, social workers, counselors, or other mental health professionals? \_\_\_\_\_

43. Have you, any family member or close friend ever been accused, arrested or convicted of a criminal offense? \_\_\_\_ YES \_\_\_\_ NO If yes, please explain: \_\_\_\_\_

44. Do you know anyone who has been confined in jail or incarcerated in prison? \_\_\_\_ YES \_\_\_\_ NO If yes, please explain: \_\_\_\_\_

45. What is your personal opinion about the military justice system (if any)? \_\_\_\_\_

46. Do you believe that the military justice system is fair? \_\_\_\_ YES \_\_\_\_ NO Please explain your answer: \_\_\_\_\_

47. What is the first thing that comes to your mind when you think of the following:  
a. Criminal Defense Attorney: \_\_\_\_\_

b. Prosecuting Attorney: \_\_\_\_\_

48. What criminal cases have you followed in the media and why did you follow those cases? \_\_\_\_\_

49. What is your opinion about the accuracy of media reports about crimes in general? \_\_\_\_\_

50. The Accused in this case is PFC Bradley Manning. The website WikiLeaks is also involved in this case. Do you know, or believe you know, anything about this case, from any source, including the newspaper, radio, television, or discussions with others? \_\_\_\_ YES \_\_\_\_ NO If yes, from which sources, what have you heard, read, seen, or talked about concerning this case and what is your reaction to that information? \_\_\_\_\_

51. Based on what you have heard, read, seen, or discussed concerning this case, have you formed any opinions concerning the people involved in this case? \_\_\_\_ YES \_\_\_\_ NO If yes, please explain those opinions: \_\_\_\_\_

---

---

52. Based on what you have heard, read, seen, or discussed concerning this case, have you formed any opinions on how the case is being handled and what the outcome should be? \_\_\_\_ YES \_\_\_\_ NO If yes, please explain those opinions: \_\_\_\_\_

---

---

53. Have you ever counseled a Soldier regarding his/her sexual preference? \_\_\_\_ YES \_\_\_\_ NO If yes, please explain when and what prompted your counseling of the Soldier: \_\_\_\_\_

---

---

54. Have you ever initiated administrative separation against a Soldier based on his/her sexual preference? \_\_\_\_ YES \_\_\_\_ NO If yes, please explain when, why, and what happened to the Soldier: \_\_\_\_\_

---

---

55. Have you ever recommended separation of a Soldier based on his/her sexual preference? \_\_\_\_ YES \_\_\_\_ NO If yes, when and approximately how many times? \_\_\_\_\_

---

---

56. Do you agree with the repeal of DADT? Why or why not? \_\_\_\_\_

---

57. Have you seen any negative impact from the repeal of DADT? \_\_\_\_ YES \_\_\_\_ NO If yes, what have you seen? \_\_\_\_\_

---

---

58. Have you seen any positive impact from the repeal of DADT? \_\_\_\_ YES \_\_\_\_ NO If yes, what have you seen? \_\_\_\_\_

---

---

59. Are any members of your immediate family homosexual? \_\_\_\_ YES \_\_\_\_ NO

60. Are any of your close friends homosexual? \_\_\_\_ YES \_\_\_\_ NO

61. What do you think when you see a cross-dresser on the street? \_\_\_\_\_

---

62. Have you worked with Department of State personnel? \_\_\_\_ YES \_\_\_\_ NO If yes, when and where?

What was your attitude towards Department of State personnel? \_\_\_\_\_

63. Please rank in order of importance to you the following purposes for punishment in a criminal case (1 being the most important and 5 being the least important):

\_\_ Closure \_\_ Deterrence \_\_ Punishment \_\_ Rehabilitation \_\_ Revenge

Please explain your answer: \_\_\_\_\_

For the following four statements, please indicate whether you strongly agree, moderately agree, slightly agree, strongly disagree, moderately disagree, or slightly disagree and explain your answer:

64. An Accused's motive in committing a crime is relevant to punishment: \_\_\_\_\_

65. If the case is a high profile case, it is important to ensure the punishment is severe to send the appropriate message: \_\_\_\_\_

66. A person should receive a harsh sentence in order to deter others from committing a similar offense: \_\_\_\_\_

67. It is possible that a criminal act can actually provide a benefit to an individual or a group of people: \_\_\_\_\_

68. As a result of your having been asked to fill out this questionnaire, have you formed any opinions about this case? \_\_\_\_ YES \_\_\_\_ NO If yes, what opinions? \_\_\_\_\_

69. Is there anything that was not asked that you believe is important to know about you? \_\_\_\_ YES \_\_\_\_ NO If yes, please explain? \_\_\_\_\_

70. Is there anything that you would like to discuss privately with the court? \_\_\_\_ YES \_\_\_\_ NO If yes, please explain? \_\_\_\_\_

71. Please provide any updated contact information:

Duty Phone: \_\_\_\_\_

Home Phone: \_\_\_\_\_

Cellular Phone: \_\_\_\_\_

E-mail address: \_\_\_\_\_

\_\_\_\_\_  
Signature

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

**DEFENSE MOTION TO  
COMPEL PRODUCTION  
OF WITNESSES AND EVIDENCE  
FOR ARTICLE 13 MOTION**

**MANNING, Bradley E., PFC** )

U.S. Army, [REDACTED] )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

DATED: 13 July 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law and Rule for Courts Martial (RCM) 703(b)(1) and 703(f)(1), requests this Court to compel production of the below listed witnesses and evidence.

BACKGROUND

2. On 29 May 2010, PFC Manning was detained by agents from the Army's Criminal Investigation Division (CID). The CID agents held PFC Manning in a secured area on Forward Operating Base Hammer, Iraq until he could be transported to the Theater Field Confinement Facility (TFCF) at Camp Arifjan, Kuwait. After 59 days, PFC Manning was transported from the TFCF and arrived at Marine Corps Base Quantico (MCBQ) Pretrial Confinement Facility (PCF) on 29 July 2010.

3. Once at the MCBQ PCF, PFC Manning was placed in Maximum (MAX) custody and under the special handling instructions of Suicide Risk (SR). Over the course of the following few weeks, PFC Manning was seen and treated by mental health professionals at the PCF. On 6 August 2010, one of these professionals, Capt. William Hocter, determined that PFC Manning was no longer a suicide risk. Capt. Hocter recommended that PFC Manning be moved from Suicide Risk to Prevention of Injury (POI) status. On 11 August 2010, the PCF commander, CWO4 James Averhart directed PFC Manning be moved from Suicide Risk to POI.

4. Over the course of the following three weeks, PFC Manning was observed by the Brig staff and received regular treatment from the Brig psychiatrists. PFC Manning did not receive any disciplinary reports or adverse spot evaluations; he was respectful, courteous and well spoken; and was evaluated as an average detainee that presented no problems to the staff or other inmates.

5. On 27 August 2010, Capt. Hocter determined that PFC Manning was no longer considered a risk of self-harm. Capt. Hocter recommended that PFC Manning be taken off of POI status and

that his confinement classification be changed from MAX to Medium Detention-In (MDI). The PCF Commander did not follow Capt. Hocter's recommendation.

6. Over the course of the next eight months, Capt. Hocter as well as other mental health professionals made recommendations to remove PFC Manning from POI status. Despite their consistent and repeated recommendations, PFC Manning remained in MAX and POI. On two occasions, the Brig placed PFC Manning on MAX and SR. The upgrade of PFC Manning from POI to SR was done over the recommendations of PCF mental health professionals.

7. PFC Manning filed several complaints regarding his custody status of MAX and POI. He filed a complaint directly to CWO4 Averhart; filed an RCM 305(g) request to the Special Court-Martial Convening Authority; filed an Article 138, Uniform Code of Military Justice (UCMJ) complaint; and sought to complain to Mr. Juan Méndez, the United Nations (UN) Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment. All of PFC Manning's efforts were unsuccessful.

### ARGUMENT

8. The Defense's Article 13, UCMJ, motion will be filed on 27 July 2012. Although the Court does not have the benefit of the Defense's motion, the underlying facts, and the supporting documentation at this time, the Defense nonetheless requests that the Court grant the Defense's motion to compel production of these witnesses because their testimony is relevant and necessary to the motion at issue.

9. The Defense has been eminently reasonable in its request for witnesses. It has only requested that a total of *seven* witnesses be produced in support of its motion. Given the duration of the unlawful pretrial punishment (approximately 8 months) and the number of witnesses that the Defense could potentially have called (several dozen), the Defense finds it disingenuous that the Government would resist production of these two witnesses. Let it remind the Government, the Government plans on calling twenty-two witnesses from the Department of State alone.

10. The Defense should be entitled to present its theory or theories of pretrial punishment in the manner of its choosing. That the Government does not agree with the theory, or the evidence presented, is of no moment. The Government can ultimately argue that the evidence is not persuasive or does not convincingly support the Defense's argument. However, that does not mean that the Defense should not be entitled to present that evidence to the Court.

11. There is an asymmetry in the military justice system, whereby the Government can call any witness that it would like in support of its motions – while the Defense must “run its witnesses by the Government” for the Government's approval. This must, of course, ultimately rest on the good faith of the prosecutor to not willy-nilly challenge Defense witnesses in order to: a) erect unnecessary hurdles for the Defense; and b) to use the challenges to flush out the Defense's theory before its time. Here, there was no reason for the Government to oppose production of these two particular witnesses. Their testimony is facially relevant to the unlawful pretrial punishment issue. Moreover, the Defense suspects that the Government will likely call at least

double the number of witnesses that the Defense has put on its witness list to rebut allegations of unlawful pretrial punishment. The stark imbalance cannot be tolerated.

**A. The Government Must Produce All Witnesses and Evidence Relevant and Necessary to the Defense.**

12. The Defense is entitled to production of witnesses whose testimony “would be relevant and necessary” to a matter in issue. RCM 703(b)(1). In determining relevance of the witness, a court must turn to the Military Rules of Evidence. *See, e.g., United States v. Breeding*, 44 M.J. 345, 351 (C.A.A.F. 1996). A witness is necessary when the witness is not cumulative, and when the witness would contribute to a party’s presentation of the case in some positive way on a matter in issue.” *United States v. Credit*, 8 M.J. 190, 193 (CMA 1980); *see also United States v. Williams*, 3 M.J. 239 (C.M.A. 1977).

**i. LTC Dawn Hilton**

13. LTC Hilton is the commander of the Fort Leavenworth Joint Regional Correctional Facility (JRCF). LTC Hilton can describe the process of PFC Manning being transferred from the MCBQ PCF to the JRCF on 19 April 2011. She can discuss the nine days PFC Manning spent going through the normal indoctrination process. She can also discuss why, after completing the indoctrination process, PFC Manning was held in medium custody with all privileges of a normal pretrial detainee. LTC Hilton can testify regarding the JRCF’s determination that PFC Manning did not need to be held in a POI status. Finally, LTC Hilton can testify regarding PFC Manning’s behavior since being held in medium custody status. Specifically, that PFC Manning has not engaged in any self-harm behavior, engaged in any assaultive behavior towards the guards, or made any attempt to escape from custody.

14. Contrary to the Government’s representation to the Court, LTC Hilton is not being called by the Defense to question another commander’s decision at a different confinement facility. Additionally the Government wholly misses the mark when it believes LTC Hilton is not relevant because the Defense “does not allege that the accused’s confinement at the JRCF violated Article 13.” *See* Appellate Exhibit CXCV at 1-2. The Government, in bad faith, also uses its opportunity to oppose the production of LTC Hilton to bring up an incident between PFC Manning and another pretrial detainee on 10 December 2011. The Government fails to note that this incident occurred eight months after PFC Manning’s arrival at the JRCF and in response to a verbal threat. The Government also does not mention how PFC Manning was reprimanded for his conduct but then was subsequently returned to medium custody with all normal privileges. The Government also fails to mention that the other pretrial detainee involved in the altercation was a repeated disciplinary problem and spent the majority of his remaining time in administrative segregation.

15. “Relevant evidence” means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence. MRE 401. LTC Hilton’s testimony is directly relevant to one aspect of the Defense’s theory of why PFC Manning’s confinement at the MCBQ PCF constituted unlawful pretrial punishment. The Defense will present evidence that PFC

Manning's custody status at the MCBQ PCF was the result of a direct order by Col. Robert G. Oltman, the Security Battalion Commander and senior rater of the Brig Commander, CWO4 James Averhart. Although the Defense believes Col. Oltman may deny giving this order, a subsequent reiteration of this order was witnessed by Capt. Hocter and Capt. Brian Moore. The fact that PFC Manning was immediately downgraded to Medium Custody with no POI restrictions after completing his indoctrination period at the JRCF makes it more likely that his custody status while at the MCBQ PCF was not for a legitimate non-punitive basis. In other words, the fact that PFC Manning went from MAX and POI at MCBQ to Medium Custody (with no POI restrictions) at the JRCF virtually overnight is evidence that he was improperly held in MAX and POI to begin with. Courts are permitted to consider after-the-fact events to determine the reasonableness and legitimacy of custodial classifications. See *United States v. Kinzer*, 56 M.J. 739, 741 (N-M. Ct. Crim. App. 2001) ("The fact that the appellant was released from special quarters the very next day after securing a pretrial agreement that limited his post-trial confinement to only three years is strong evidence that his assignment to special quarters was based primarily upon a length-of-sentence policy, and not upon other appropriate factors. Accordingly, we find that the decision to place the appellant in special quarters was based on an arbitrary policy and resulted in the imposition of conditions more rigorous than necessary to insure his presence for trial.").

16. The Defense does not object to LTC Hilton testifying by telephone. RCM 703(b)(1) (stating that the military judge may authorize any witness to testify via remote means).

**ii. Mr. Juan Méndez**

17. Mr. Méndez is the United Nations Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment. Mr. Méndez will testify about his communications with the U.S. Government regarding the confinement conditions of PFC Manning. He will testify that he was told that the confinement conditions were imposed on PFC Manning due to the seriousness of the offenses. He will also testify that the U.S. Government informed him that PFC Manning was not being held in "solitary confinement" but was being held in "prevention of harm watch" but would not offer any details about what harm was being prevented by such a status. He will also testify regarding his efforts to meet with PFC Manning for an unmonitored conversation. Despite his numerous requests, he will testify that he was informed that his conversation would be monitored. Mr. Méndez will testify that the U.S. Government's refusal to allow unmonitored conversations with PFC Manning violates international norms and U.N. requirements, as documented in an official report he prepared. Due to the U.S. Government's continued refusal to allow unmonitored conversations, Mr. Méndez had to decline the opportunity to meet with PFC Manning. Mr. Méndez will also testify that he was aware, through Mr. Coombs, that PFC Manning also believed that an unmonitored meeting was not in his best interests. The reason unmonitored visits were not in PFC Manning's best interest was due to the fact that he would likely face a reprisal for anything that he said to Mr. Méndez.

18. Contrary to the Government's representation to the Court, Mr. Méndez did not decline to meet with PFC Manning due to PFC Manning's refusal to have an unmonitored conversation. The attached report by Mr. Méndez clearly states:



The US Government authorized the visit but ascertained that it could not ensure that the conversation would not be monitored. Since a non-private conversation with an inmate would violate the terms of reference applied universally in fact-finding by Special Procedures, *the Special Rapporteur had to decline the invitation.*

See Attachment A (emphasis added).

19. "Relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence. MRE 401. Mr. Méndez's testimony is directly relevant to several aspects of the Defense's unlawful pretrial punishment argument. First, the Defense will use Mr. Méndez's testimony's to support its argument that PFC Manning was held under unduly onerous confinement conditions owing solely to the seriousness of the charges against him. Officials told Mr. Méndez that this was the primary reason for the onerous conditions of PFC Manning's confinement. Second, the Defense will argue that the failure to allow PFC Manning to have access to Mr. Méndez for an unmonitored visit where PFC Manning could freely discuss the conditions of his confinement in the hopes of getting some type of reprieve from them *itself* amounts to unlawful pretrial punishment. Because everyone at the MCBQ PCF was abiding by Col. Oltman's unlawful order to not remove PFC Manning from MAX or POI, there was nowhere for PFC Manning to go – other than outside the chain of command – to potentially get relief. Case law has repeatedly emphasized the importance of the accused seeking out any and all forms of relief in an Article 13 claim. The failure to permit PFC Manning an unmonitored visit with the UN Special Rapporteur on Torture was designed to cover up from public view the wrongs that were being perpetrated at MCBQ. Extensive documentation will be introduced showing how brig rules were being deliberately read in an absurd manner (by both the Government and officials at MCBQ) in order to deny Mr. Méndez's visit. Third, Mr. Méndez will testify that the Government's refusal to allow unmonitored visits was surprising to him and was in violation of international norms. Mr. Méndez will also testify generally about his knowledge of solitary confinement being in violation of international law. The Defense believes that Mr. Méndez's testimony regarding international norms speaks to the issue of whether there was pretrial punishment and also speaks to the appropriate remedy for such punishment (i.e. conduct that is so egregious that it rises to the level of a violation of international law warrants a greater remedy than a simple breach, say, of brig regulations).

20. Mr. Méndez has volunteered to testify. He resides in Washington D.C. and would not present a significant cost to the Government nor would his presence result in a delay in the proceedings.

## **ii. Requested Evidence**

21. The Defense has requested that the Government produce three pieces of evidence for the Court's consideration: the issued suicide prevention smock, suicide prevention blanket, and suicide prevention mattress. RCM 703(f)(4)(A). Each piece of requested evidence can be obtained from MCBQ.

22. The requested evidence is directly relevant to the defense's theory of why PFC Manning's confinement at the MCBQ PCF constituted unlawful pretrial punishment. Each piece of evidence will independently demonstrate an aspect of the onerous conditions PFC Manning was unnecessarily subjected to while at MCBQ PCF. The requested evidence will also demonstrate how PFC Manning was held under conditions more rigorous than necessary to ensure his presence for trial. PFC Manning was subjected to each of the requested evidentiary items due to the MCBQ PCF's determination to hold him either on SR or POI status from 29 July 2010 to 19 April 2011.

23. Shortly after the deciding to strip PFC Manning of all of his clothing at night on 2 March 2011 (something that the Defense submits itself amount to unlawful punishment), the MCBQ PCF decided to require PFC Manning to wear a suicide prevention article of clothing called a "smock" at night. Due to PFC Manning's size and the coarseness of the smock, he had difficulty sleeping. The suicide smock that he was required to wear was not designed for someone of his size. It is important for the Court to see the smock in relations to PFC Manning's size to assess the reasonableness of this restriction.

24. Additionally, the smock itself posed a risk of harm to PFC Manning. On one occasion, PFC Manning got trapped inside the smock. The situation is explained in an Incident Report on 13 March 2011:

Ma'am, on the above date and time while performing my duties as special quarters supervisor, I, LCPL Miller, noticed Det. Manning [REDACTED] had his head and arms inside of his POI jump suit. I then woke up SND and told him that I need to see his face and to poke his head out. While doing what I instructed him to do, SND realized he was stuck and began to roll around, saying, "I hate this stupid thing." I then told SND to calm down and stand up and try to pull the POI jump suit over his head, but his arms were still stuck. I then called for the watch supervisor, CPL Sanders, to come down to special quarters to look at the situation and get permission to open cell 191 and help SND. Upon CPL Sanders arrival, he evaluated the situation and opened cell 191 to help SND free his arms. Once SND was situated, I then told him not to put his head and arms inside his POI jump suit again, and that if he is cold to use his second POI blanket instead. The DBS was then notified and this report was written, and the incident was recorded on camera.

*See Attachment B.*

25. The Brig psychiatrists did not believe the smock precaution was needed and had consistently determined that PFC Manning was not a risk of self harm. Nonetheless, the MCBQ PCF commander, then CWO2 Denise Barnes, refused to change the decision to require PFC Manning to surrender his clothing and wear a smock at night. Her decision was not based upon a legitimate non-punitive basis, and thus constituted an additional aspect of unlawful pretrial punishment at the hands of MCBQ PCF.

26. PFC Manning was also not allowed to have a pillow or sheets. Instead he was provided with a suicide prevention mattress with a built-in pillow and a tear proof suicide prevention blanket. The provided mattress was uncomfortable and difficult for PFC Manning to sleep on. Additionally, the suicide prevention blanket was coarse and would frequently cause either a rash or a burn to PFC Manning's skin. As with the suicide smock, the Brig psychiatrists did not believe the suicide prevention measures of the mattress and tear proof blanket were necessary.

27. Contrary to the Government's representation to the Court, a picture of the above requested items will not be sufficient for the Court to "understand its purpose, limitations, or possible effect." See Appellate Exhibit CXCv at 2. The requested evidence is under the control of the Government. The requested production is not unreasonable or oppressive. As such, the Defense's request should be granted.

#### CONCLUSION

28. For the above reasons, the Defense requests this Court compel production of the above listed witnesses and evidence.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'David E. Coombs', with a stylized flourish at the end.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

# ATTACHMENT A

## United Kingdom of Great Britain and Northern Ireland

- (a) UA 23/02/2011 Case No. GBR\_1/2011 State reply: None to date Alleged risk of torture for asylum seeker facing deportation.

168. The Special Rapporteur regrets that the Government of the United Kingdom of Great Britain and Northern Ireland has not responded to this communication, thereby failing to cooperate with the mandate issued by the Human Rights Council. The communication referred to allegations of risk of torture for Mr. X, a homosexual man, if returned to Burundi. The Special Rapporteur reiterates that article 3 of the UN Convention against Torture holds that no State party shall expel, return ("refouler"), or extradite a person to another State where there are substantial grounds for believing that the person would be in danger of being subjected to torture. Based on the information received, the Special Rapporteur determines that the rights of Mr. X under the UN Convention against Torture are at risk of being violated. The Special Rapporteur calls on the Government not to extradite Mr. X until a fair assessment of his risk of torture is conducted. In this context, diplomatic assurances do not mitigate the Government's obligation to refrain from violating the non-refoulement provision.

- (b) JAL 11/11/2011 Case No. GBR\_6/2011 State reply: 13/01/2012 26/01/2012 Concerns regarding the remit and conduct of the forthcoming United Kingdom of Great Britain and Northern Ireland (UK) Detainee Inquiry.

169. The Special Rapporteur is grateful to the Government for its responses to this communication. Given the on-going dialogue between the mandate and the Government on this case, the Special Rapporteur decides not to make observations on this case in the present report.

## United States of America

- (a) UA 30/12/2010 Case No. USA\_20/2010 State reply: 27/01/2011 19-05/2011 Allegations of prolonged solitary confinement of a soldier charged with the unauthorized disclosure of classified information.

170. The Special Rapporteur thanks the Government of the United States of America for its response to this communication regarding the alleged prolonged solitary confinement of Mr. Bradley E. Manning, a US soldier charged with the unauthorized disclosure of classified information. According to the information received, Mr. Manning was held in solitary confinement for twenty-three hours a day following his arrest in May 2010 in Iraq, and continuing through his transfer to the brig at Marine Corps Base Quantico. His solitary confinement - lasting about eleven months - was terminated upon his transfer from Quantico to the Joint Regional Correctional Facility at Fort Leavenworth on 20 April 2011. In his report, the Special Rapporteur stressed that "solitary confinement is a harsh measure which may cause serious psychological and physiological adverse effects on individuals regardless of their specific conditions". Moreover, "[d]epending on the specific reason for its application, conditions, length, effects and other circumstances, solitary confinement can amount to a breach of article 7 of the International Covenant on Civil and Political Rights, and to an act defined in article 1 or article 16 of the Convention against Torture." (A/66/268 paras. 79 and 80). Before the transfer of Pfc Manning to Fort Leavenworth, the Special Rapporteur requested an opportunity to interview him in order to ascertain the precise conditions of his detention. The US Government authorized the visit but ascertained that it could not ensure that the conversation would not be monitored. Since a non-private conversation with an inmate would violate the terms of reference applied universally in fact-finding by Special Procedures, the Special Rapporteur had to decline the invitation. In

response to the Special Rapporteur's request for the reason to hold an undicted detainee in solitary confinement, the government responded that his regimen was not "solitary confinement" but "prevention of harm watch" but did not offer details about what harm was being prevented. To the Special Rapporteur's request for information on the authority to impose and the purpose of the isolation regime, the government responded that the prison rules authorized the brig commander to impose it on account of the seriousness of the offense for which he would eventually be charged. The Special Rapporteur concludes that imposing seriously punitive conditions of detention on someone who has not been found guilty of any crime is a violation of his right to physical and psychological integrity as well as of his presumption of innocence. The Special Rapporteur again renews his request for a private and unmonitored meeting with Mr. Manning to assess his conditions of detention.

- (b) AL 15/06/2011 Case No. USA 8/2011 State reply: None to date Follow-up to a letter sent 13 May 2011 requesting a private unmonitored meeting with Private (Pfc.) Bradley Manning.

171. The Special Rapporteur thanks the Government of the United States of America for its response to the communication dated 13 May 2011 requesting a private unmonitored meeting with Private Bradley Manning. Regrettably, to date the Government continues to refuse to allow the Special Rapporteur to conduct private, unmonitored, and privileged communications with Private Manning, in accordance with the working methods of his mandate (E/CN.4/2006/6 paras. 20-27).

- (c) JUA 19/08/2011 Case No. USA 15/2011 State reply: None to date Alleged torture and ill-treatment in immigration facilities.

172. The Special Rapporteur regrets that the Government of the United States of America to date has not responded to the communication dated 19 August 2011, regarding the allegations of torture and ill-treatment in immigration facilities. According to the information received, 16 gay and transgender individuals have allegedly been subjected to solitary confinement, torture and ill-treatment while in detention in U.S. immigration facilities. Furthermore, there was reportedly a lack of protection from persecution and respect for the principle of non-refoulement for those who risk torture if returned to their home countries on account of their sexual orientation, gender identity or HIV status. In this regard, the Special Rapporteur would like to draw the attention of the Government to paragraph 6 of General Comment No. 20 of the Human Rights Committee, to article 7 of the Basic Principles for the Treatment of Prisoners, to the Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment and the Standard Minimum Rules for the Treatment of Prisoners, particularly rule 22 (2). Given the lack of any evidences to the contrary, the Special rapporteur believes that the fact reveal that there have been various violations of the provisions under the Convention against Torture, in particular breach of articles 7 and 12. The Special Rapporteur calls on the Government to undertake a prompt and impartial investigation on the conditions of detention, solitary confinement and ill-treatment of the immigrants, prosecute and punish those responsible, and ensure that the victims obtain redress, including fair and adequate compensation, and as full rehabilitation as possible.

- (d) AL 16/09/2011 Case No. USA 16/2011 State reply: 30/11/2011 Alleged widespread use of solitary confinement, including its prolonged and indefinite use and the imposition of solitary confinement on individuals with mental disabilities.

173. The Special Rapporteur is grateful that the Government of the United States of America replied to the allegation letter of 16 September 2011. Considering the on-going dialogue on the issues raised between the mandate and the Government, the Special Rapporteur decides not to make observations on this case in the present report. He encourages the Government to continue its engagement with the mandate.

# ATTACHMENT B

INCIDENT REPORT (CORRECTIONAL FACILITY)  
MCBQ-5520/10 (Rev. 6-83)

Complete this form in TRIPLICATE. Ensure that all information is CORRECT and LEGIBLE. Forward original and one copy to the Administration Chief. One copy is to be retained by the Security Chief or OIC of the individual's organization if the incident occurred outside the facility.

LOCATION OF INCIDENT		TIME	DATE
MARINE CORPS BASE PRETRIAL CONFINEMENT FACILITY		0010	20110313
INDIVIDUAL(S) INVOLVED			
ID NUMBER	NAME (LAST, FIRST, MI)	LOCATION/DORM	INJURED (YES/NO)
10075	MANNING	SQ	NO
DUTY STATUS - Light Duty, No Duty, Bed Rest, Admitted NRMCC, Other			

DESCRIPTION OF INCIDENT AND ACTION TAKEN (USE REVERSE IF NEEDED)

MAAM, ON THE ABOVE DATE AND TIME WHILE PERFORMING MY DUTIES AS SPECIAL QUARTERS SUPERVISOR I, LCPL MILLER, NOTICED DET MANNING [REDACTED] HAD HIS HEAD AND ARMS INSIDE OF HIS POI JUMP SUIT. I THEN WOKE UP SNO AND TOLD HIM THAT I NEED TO SEE HIS FACE AND TO POKE HIS HEAD OUT. WHILE DOING WHAT I INSTRUCTED HIM TO DO, SNO REALIZED HE WAS STUCK AND BEGAN TO ROLL AROUND SAYING, "I HATE THIS STUPID THING." I THEN TOLD SNO TO CALM DOWN AND STAND UP TO TRY TO PULL THE POI JUMP SUIT OVER HIS HEAD, BUT HIS ARMS WERE STILL STUCK. I THEN CALLED FOR THE WATCH SUPERVISOR, CPL SANDERS, TO COME DOWN TO SPECIAL QUARTERS TO LOOK AT THE SITUATION AND GET PERMISSION TO OPEN CELL 191 AND HELP SNO. UPON CPL SANDERS ARRIVAL HE EVALUATED THE SITUATION AND OPENED CELL 191 TO HELP SNO FREE HIS ARMS. ONCE SNO WAS SITUATED I THEN TOLD HIM NOT TO PUT HIS HEAD AND ARMS INSIDE HIS POI JUMP SUIT AGAIN, AND THAT IF HE IS COLD TO USE HIS SECOND POI BLANKET INSTEAD. THE DBS WAS THEN NOTIFIED AND THIS REPORT WAS WRITTEN, AND THE INCIDENT WAS RECORDED ON CAMERA. EOS.

R/S  
MILLER SR., J. E.  
*John Miller*  
LCPL USMC/ SEC II

TIME AMBULANCE CALLED	TIME SENT TO SICK BAY	TIME SENT TO HOSPITAL	TIME RETURNED TO FACILITY
N/A	N/A	N/A	N/A
FOLLOWING PERSONS NOTIFIED			
NAME OF PERSON MAKING CALLS			TIME
N/A			0010
TITLE	NAME	TIME	
ADMIN CHIEF	SGT GARNETT	110314/1825	
PROGRAMS CHIEF	GYSGT BLENIS	110314/0730	
OPERATIONS CHIEF	GYSGT FULLER		
BRIG SUPERVISOR	MSGT PAPAIE	110314 0830	
BRIG COMMANDER	CWO2 BARNES	110314/1434	
NAME, GRADE, ORGANIZATION TITLE (PRINT)	SIGNATURE	TIME	DATE
LCPL MILLER	<i>John Miller</i>	0010	20110313
THIS REPORT RECEIVED IN ADMIN OFFICE BY	SIGNATURE	TIME	DATE

MCBQ-5520/10 (Rev. 6-83)

FOR OFFICIAL USE ONLY

PROPERTY



## TO PROSPECTIVE MEMBERS

This questionnaire is designed to obtain information from you with respect to your qualifications to sit as a member in this case. By the use of the questionnaire, the process of member selection will be shortened.

Please do not discuss any of these questions or your answers with any other prospective members. Please respond to the following questions as completely as possible.

The answers to these questions will be used by the Court and the attorneys solely for the selection of the panel members in this case and for no other reason. The information contained within the questionnaire will become part of the Court's permanent record, but it will not be distributed to anyone except the attorneys in the case and the Judge.

During the later questioning by the attorneys, you will be given an opportunity to explain or expand any of your answers, if necessary. If there are any answers or explanations you would prefer to answer in private, please write the word, "**PRIVATE**" next to the question. If you do not understand a question, please write "**I DO NOT UNDERSTAND**" and the question will be explained to you. If your answers or explanations to any question will not fit completely in the space provided, please use the back of the page, making sure to indicate in the space provided under the question that you have continued your answer on the back. In addition, please make sure to write the number of the question/answer you are completing with the remainder of your answer.

MEMBER NUMBER: \_\_\_\_\_

DATE PREPARED: \_\_\_\_\_

**COURT-MARTIAL MEMBER QUESTIONNAIRE**  
**(PLEASE PRINT CLEARLY & USE BLACK INK)****BACKGROUND**

1. Full name: \_\_\_\_\_  
(First) (Middle) (Last) (Maiden, if applicable)
2. Date of birth: \_\_\_\_\_ Age: \_\_\_\_\_ Sex: \_\_\_\_\_ Race: \_\_\_\_\_  
Birthplace (City/Town & State): \_\_\_\_\_
3. Please provide the following information for any other locations at which you have lived in the past three years:

DATES	TOWN/CITY, STATE, COUNTRY	LENGTH OF RESIDENCE

**MILITARY SERVICE**

4. Current duty station and office telephone number: \_\_\_\_\_  
\_\_\_\_\_
5. Rate/rank: \_\_\_\_\_ Date of rate/rank: \_\_\_\_\_
6. MOS: \_\_\_\_\_  
Job title, description and duties: \_\_\_\_\_  
\_\_\_\_\_  
Length of present assignment: \_\_\_\_\_  
Name and title of supervisor: \_\_\_\_\_
7. Do you now have, or have you ever had the authority to train, supervise, assign, evaluate, or discipline others? ☐ YES ☐ NO IF YES, Please describe your feelings concerning the importance of mentoring junior enlisted: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
8. Why do junior enlisted need to be mentored? \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

9. Have any of you ever heard the expression "with proper leadership, failure is not an option?" If so, what does that term mean to you?

---

---

---

10. Have you ever been denied a security clearance or had a security clearance revoked?  
☐ YES ☐ NO If YES, please indicate when and the reason for the denial or revocation:

---

---

11. Have you ever had seen another soldier been denied a security clearance or had a security clearance revoked?

☐ YES ☐ NO If YES, please indicate when and the reason for the denial or revocation:

---

---

---

12. Do you believe that the command should revoke a soldier's security clearance if the soldier exhibits any signs of mental or emotional instability?

☐ YES ☐ NO If YES, please indicate why:

---

---

---

13. Do you believe that the command should revoke a soldier's security clearance if the soldier exhibits any signs aggression towards other soldiers?

☐ YES ☐ NO If YES, please indicate why:

---

---

---

14. Have you ever worked as a military police, in military law enforcement or investigations?

☐ YES ☐ NO If YES, please indicate:

DATES	RANK	DUTIES

15. Were you ever involved in combat? ☐ YES ☐ NO If YES, please give dates and locations:

---

---

---

---

---

16. Do you believe that a command should deploy a soldier if the soldier exhibits signs of mental or emotional instability?

☐ YES ☐ NO If NO, please indicate why:

---

---

---

---

17. Years of active duty: \_\_\_\_\_

18. (Officers only) Source of commission: \_\_\_\_\_

19. (Officers only) Have you had any enlisted service? ☐ YES ☐ NO If YES, please indicate:

DATES	YEARS	HIGHEST RANK

#### CIVILIAN EMPLOYMENT

20. Have you ever been employed as a civilian? ☐ YES ☐ NO If YES, please indicate the following for each employment:

DATES	LENGTH OF EMPLOYMENT	NAME & NATURE OF BUSINESS	TITLE & DUTIES

#### EDUCATION

21. Is English your first language? ☐ YES ☐ NO If NO, what was your first language and when did you begin speaking English? \_\_\_\_\_
22. What is the primary language spoken in your home? \_\_\_\_\_

23. Do you have any difficulty in reading or writing the English language? ☐ Yes ☐ No If YES, please explain: \_\_\_\_\_

24. Have you attended technical or trade schools (including any military schools)? ☐ Yes ☐ No If YES, please indicate the following for each school you attended:

DATES	NAME OF SCHOOL	LOCATION (CITY/STATE)	MAJOR	MINOR	DEGREE EARNED

25. Have you attended college (**undergraduate**): ☐ Yes ☐ No If YES, please indicate the following for each undergraduate college you attended:

DATES	NAME OF SCHOOL	LOCATION (CITY/STATE)	MAJOR	MINOR	DEGREE EARNED

26. Have you attended post-graduate school? ☐ Yes ☐ No If YES, please indicate the following for each post-graduate school you attended:

DATES	NAME OF SCHOOL	LOCATION (CITY/STATE)	MAJOR	MINOR	DEGREE EARNED

27. Have you attended law school, or taken any law courses (including any Army schools)? ☐ Yes ☐ No If YES, please indicate the following for each:

DATES	NAME OF SCHOOL	LOCATION (CITY/STATE)	LENGTH	TOPIC	DEGREE EARNED

28. Have you taken any courses, seminar, or training in the following areas (**please check all that apply**):

- |   |   |  |                                     |
|---|---|--|-------------------------------------|
| <input type="checkbox"/> BIOLOGY            | <input type="checkbox"/> CHEMISTRY      | <input type="checkbox"/> CONSTITUTIONAL LAW  | <input type="checkbox"/> COUNSELING |
| <input type="checkbox"/> CRIMINAL JUSTICE   | <input type="checkbox"/> CRIMINOLOGY    | <input type="checkbox"/> CRISIS INTERVENTION | <input type="checkbox"/> EDUCATION  |
| <input type="checkbox"/> EMERGENCY RESPONSE | <input type="checkbox"/> FAMILY THERAPY | <input type="checkbox"/> LAW ENFORCEMENT     | <input type="checkbox"/> MEDICINE   |
| <input type="checkbox"/> PHARMACOLOGY       | <input type="checkbox"/> PHILOSOPHY     | <input type="checkbox"/> PSYCHOLOGY          | <input type="checkbox"/> PSYCHIATRY |
| <input type="checkbox"/> RELIGION           | <input type="checkbox"/> SOCIAL WORK    | <input type="checkbox"/> SOCIOLOGY           |                                     |

# **MARITAL STATUS & SPOUSE INFORMATION**

29. Please indicate your current personal status:

- ☐ SINGLE (NEVER BEEN MARRIED)
 ☐ SEPARATED (HOW LONG?) \_\_\_\_\_
 ☐ DIVORCED (HOW LONG?) \_\_\_\_\_
 ☐ DIVORCED/REMARRIED (HOW LONG?) \_\_\_\_\_
 ☐ WIDOWED (HOW LONG?) \_\_\_\_\_
 ☐ WIDOWED/REMARRIED (HOW LONG?) \_\_\_\_\_

30. Current and/or former spouse's employer, job title, description and duties: \_\_\_\_\_

31. Is or has your (current and/or former) spouse ever been employed as a civilian? ☐ YES ☐ NO If YES, please indicate the following for each employment during the previous five years:

DATES	LENGTH OF EMPLOYMENT	NAME & NATURE OF BUSINESS	TITLE & DUTIES

32. Has your (current and/or former) spouse ever served in any branch of the Armed Forces? ☐ YES ☐ NO If YES, please give a summary of your spouse's military career (*please include all significant or unusual jobs and service in any other branch of the Armed Forces*):

DATES	BRANCH	ENLIST/COMMISSION/REENLIST	HIGHEST RANK	DUTY STATION/COMMAND	DUTIES & SPECIFIC ASSIGNMENT	DATE/TYPE OF DISCHARGE

33. What special recognition, awards, medals or commendations did your current and/or former spouse receive? \_\_\_\_\_

34. Has your current and/or former spouse ever worked as a military police, in military law enforcement or investigations? ☐ YES ☐ NO If YES, please indicate:

DATES	RANK	DUTIES

35. Has your current and/or former spouse ever been involved in combat? ☐ YES ☐ NO If YES, please give dates and locations: \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

36. Is your current and/or former spouse a high school graduate? ☐ YES ☐ NO

37. Has your current and/or former spouse attended any technical or trade schools (including any military schools)? ☐ YES ☐ NO If YES, please indicate the following for each school attended:

DATES	NAME OF SCHOOL	LOCATION (CITY/STATE)	MAJOR	MINOR	DEGREE EARNED

38. Has your current and/or former spouse attended college (*undergraduate*): ☐ YES ☐ NO If YES, please indicate the following for each undergraduate college attended:

DATES	NAME OF COLLEGE	LOCATION (CITY/STATE)	MAJOR	MINOR	DEGREE EARNED

39. Has your current and/or former spouse attended post-graduate school? ☐ YES ☐ NO If YES, please indicate the following for each post-graduate school attended:

DATES	NAME OF SCHOOL	LOCATION (CITY/STATE)	MAJOR	MINOR	DEGREE EARNED

40. Has your current and/or former spouse attended law school, or taken any law courses (including any schools)? ☐ YES ☐ NO If YES, please indicate the following for each:

DATES	NAME OF SCHOOL	LOCATION (CITY/STATE)	LENGTH	TOPIC	DEGREE EARNED

41. Please provide the following information about each of your children, stepchildren, foster children or grandchildren:

RELATIONSHIP (SON, STEPSON, ETC.)	SEX	AGE	EDUCATION	CURRENT/LAST OCCUPATION	STATUS	LIVING IN YOUR HOME
					<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
					<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
					<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
					<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
					<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
					<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
					<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
					<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO

42. Please provide the following information about each parent, stepparent, foster parent or person who raised you:

RELATIONSHIP (FATHER, AUNT, ETC.)	AGE	EDUCATION	CURRENT/LAST OCCUPATION	STATUS	LIVING IN YOUR HOME
				<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
				<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
				<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
				<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO

43. Please provide the following information about each sibling, stepsibling, foster sibling or anyone raised with you:

RELATIONSHIP (BROTHER, COUSIN, ETC.)	AGE	EDUCATION	CURRENT/LAST OCCUPATION	STATUS	LIVING IN YOUR HOME
				<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
				<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
				<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
				<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO
				<input type="checkbox"/> LIVING <input type="checkbox"/> DECEASED	<input type="checkbox"/> YES <input type="checkbox"/> NO

#### FAMILY MILITARY SERVICE

44. Have your parents (including stepparents or foster parents) or siblings (including stepsiblings or foster siblings) ever served in any branch of the Armed Forces?

RELATIONSHIP	DATES	BRANCH	ENLIST/COMMISSION/REENLIST	HIGHEST RANK	DUTIES & SPECIFIC ASSIGNMENT



--	--	--	--	--	--

45. What special recognition, awards, medals or commendations did any of those listed above receive? \_\_\_\_\_
46. Have any of those listed above ever worked as a military police, in military law enforcement or investigations? ☐ YES ☐ NO If YES, please indicate:

RELATIONSHIP	DATES	RANK	DUTIES

47. Have any of those listed above ever been involved in combat? ☐ YES ☐ NO If YES, please give dates and locations for each: \_\_\_\_\_

#### INTERESTS & HOBBIES

48. Please list the civil clubs, societies, professional associations, or other organizations to which you now belong, or to which you have belonged in the past: \_\_\_\_\_
49. Have you ever served as an officer or held a position of leadership in any of these organizations? ☐ YES ☐ NO If YES, please explain: \_\_\_\_\_
50. To which charitable organizations do you contribute money, time, services or resources, and why did you choose those organizations? \_\_\_\_\_
51. What are your hobbies: \_\_\_\_\_
52. What do you enjoy doing in your spare time: \_\_\_\_\_
53. What were the last three books you have read: (1) \_\_\_\_\_  
(2) \_\_\_\_\_ (3) \_\_\_\_\_
54. In general, what types of books do you most often read? \_\_\_\_\_

55. Have you ever read a book about releasing classified information or any similar action? ☐ YES  
☐ NO If YES, which book, who was the author, what trial or crime and why were you interested? \_\_\_\_\_
56. What newspapers do you regularly read or subscribe to: \_\_\_\_\_
57. What magazines, journals or other periodicals do you regularly read or subscribe to: \_\_\_\_\_
58. Have you ever written a letter to the editor? ☐ YES ☐ NO If YES, about what issue did you write and why did you decide to write the letter: \_\_\_\_\_
59. Do you usually read for ☐ ENTERTAINMENT PURPOSES or for ☐ BUSINESS PURPOSES?
60. How often do you listen to the radio, which stations and which programs do you usually listen to? \_\_\_\_\_
61. Approximately how many hours per week do you spend watching television? \_\_\_\_\_
62. What television shows do you watch regularly: (1) \_\_\_\_\_  
(2) \_\_\_\_\_ (3) \_\_\_\_\_
63. What is your main source of news? \_\_\_\_\_
64. Which television news programs do you usually watch for local, state, national and world news? \_\_\_\_\_
65. Are you most interested in Local, State, National or World news? \_\_\_\_\_
66. Do you typically watch any news magazine programs (*Dateline NBC, 20/20, 60 Minutes, 48 Hours, etc.*)? ☐ YES ☐ NO If YES, which programs? \_\_\_\_\_
67. How often do you go to see a movie? \_\_\_\_\_
68. In general, what types of movies do you most prefer (i.e. romantic comedies, dramas, action, mysteries, science fiction, etc.)? \_\_\_\_\_
69. What are the last three movies you went to see: (1) \_\_\_\_\_  
(2) \_\_\_\_\_ (3) \_\_\_\_\_
70. On **social** issues, are you:

☐ VERY CONSERVATIVE   ☐ CONSERVATIVE   ☐ MODERATE   ☐ LIBERAL   ☐ VERY LIBERAL

PLEASE EXPLAIN: \_\_\_\_\_

71. Please list the 3 people you admire or respect ***the most*** and tell us ***why***:

- (1) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
(2) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
(3) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

72. Please list the 3 people you admire or respect ***the least*** and tell us ***why***:

- (1) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
(2) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
(3) \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

73. Please list the one ***person*** you feel most influenced your life, either positively or negatively, and tell us ***why***: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

74. Please list the one ***event*** you feel most influenced your life, either positively or negatively, and tell us ***why***: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

#### YOUNG INDIVIDUALS

75. Do you have any children? ☐ YES ☐ NO If YES, please indicate the gender and age of each of your children. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

76. Does anyone believe that young individuals are susceptible to make mistakes in judgment?  
☐ YES ☐ NO Please indicate why you feel this way. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

77. Does anyone believe that the legal drinking age should be lower than 21 years of age?  
☐ **YES** ☐ **NO** Please indicate why you feel this way. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
78. Does anyone believe that 21 is too young for a person to get married? ☐ **YES** ☐ **NO**  
Please indicate why you feel this way. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
79. Why do you believe that rental car companies do not rent cars to individuals under the age of 25? \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
80. Have you ever heard the expression "kids these days think that they know it all?"  
☐ **YES** ☐ **NO** If Yes, what does this expression mean to you? \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
81. Do you believe that the typical 20 something-year-old believes that they "know it all?"  
☐ **YES** ☐ **NO** Please indicate why you feel this way. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
82. Do believe that it is not unusual for a person in their early twenties to believe that they can do something to make a difference or change the world? ☐ **YES** ☐ **NO** Please indicate why you feel this way. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**RELIGION**

83. On *religious* issues, do you consider yourself to be:  
☐ **VERY CONSERVATIVE** ☐ **CONSERVATIVE** ☐ **MODERATE** ☐ **LIBERAL** ☐ **VERY LIBERAL**  
**PLEASE EXPLAIN:** \_\_\_\_\_  
\_\_\_\_\_

POLITICAL

84. Are you a registered voter? ☐ YES ☐ NO Do you vote regularly? ☐ YES ☐ NO
85. During which elections do you usually vote (*please select all that apply*):  
☐ LOCAL ☐ STATE ☐ NATIONAL
86. On *political* issues, do you consider yourself to be:  
☐ VERY CONSERVATIVE ☐ CONSERVATIVE ☐ MODERATE ☐ LIBERAL ☐ VERY LIBERAL  
**PLEASE EXPLAIN:** \_\_\_\_\_

87. Have you ever signed a petition? ☐ YES ☐ NO If YES, please tell us what were the issue(s): \_\_\_\_\_
88. Have you ever participated in a march, protest or demonstration? ☐ YES ☐ NO If YES, please tell us when and what were the issue(s): \_\_\_\_\_

PSYCHOLOGY

89. Have you or any family members or close friends ever worked in the mental health or related field (psychiatrist, psychologist, psychiatric nurse, social worker, counselor, etc.)? ☐ YES ☐ NO  
If YES, please tell us who, when and what that person's job duties included: \_\_\_\_\_
90. Have you ever read books or articles dealing with psychiatry, psychology, social work or mental health issues? ☐ YES ☐ NO If YES, please tell us which books, when and why you read them: \_\_\_\_\_
91. Have you ever taken any courses or seminars in the fields of psychiatry, psychology, social work or counseling? ☐ YES ☐ NO If YES, please tell us what courses, when and why you took those courses or seminars: \_\_\_\_\_
92. What are your thoughts, feelings or opinions, in general, about psychiatrists, psychologists, social workers, counselors or other mental health professionals? \_\_\_\_\_
93. Do you know any psychiatrists, psychologists, social workers or counselors on a personal or professional basis? ☐ YES ☐ NO If YES, please tell us who, what type of work they do and

the nature of your relationship with that person: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

94. Have you ever known anyone who you believe suffered from severe emotional problems?

☐ YES ☐ NO If YES, please explain: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

95. Have you or any family members or any close friends ever undergone counseling, treatment, or hospitalization for psychiatric, emotional, family, or behavioral problems? ☐ YES ☐ NO If YES, please tell us who and provide the details, including the name of the hospital, doctor or counselor seen, diagnosis, treatment and outcome: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

96. Have you followed any criminal cases that involved testimony about severe emotional problems experienced by the person accused of a crime? ☐ YES ☐ NO If YES, what was the case, why did you follow it, what was the outcome and what were your feelings about the outcome? \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

#### **ABUSE**

97. Have you or any family members or close friends ever volunteered time, money, services, materials, etc. to any children's protective service, crisis intervention, emergency response, emergency medical care, fire department, search and rescue, shelters, or any organizations involved in helping victims of abuse, in general? ☐ YES ☐ NO If YES, who was involved, how was that person involved and why did that person become involved? \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

98. Have you or any member of your family or friends ever used any of the above services?

☐ YES ☐ NO If YES, please explain: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

99. Do you know anyone who has experienced any type of abusive relationship (sexual abuse, physical abuse, verbal abuse, emotional/psychological abuse, etc.)? ☐ YES ☐ NO If YES, please explain: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

100. If a person experiences abuses as a child, how do you believe that might impact their social abilities with others as a young adult? \_\_\_\_\_

**CRIME**

101. Have you, any family member or close friend ever been accused, arrested or convicted of a criminal offense? ☐ YES ☐ NO If YES, please explain: \_\_\_\_\_
102. Do you know anyone who has been in jail or who has been to prison? ☐ YES ☐ NO If YES, please explain: \_\_\_\_\_
103. Do you believe that there are some serious crimes where a lengthy jail sentence would serve no legitimate purpose? ☐ YES ☐ NO If YES, please explain: \_\_\_\_\_

**MILITARY JUSTICE SYSTEM**

104. What is your personal opinion about the military justice system? \_\_\_\_\_
105. Do you believe the military justice system is fair? ☐ YES ☐ NO *PLEASE EXPLAIN YOUR ANSWER:* \_\_\_\_\_
106. Do you believe the military justice should be influenced by outside civilian pressures to send a message in certain cases? ☐ YES ☐ NO *PLEASE EXPLAIN YOUR ANSWER:* \_\_\_\_\_

**MILITARY LAW**

107. Have you ever served as summary court-martial officer? ☐ YES ☐ NO If YES, please provide information about when, the cases and results: \_\_\_\_\_

108. Have you ever convened (as OIC/Commanding Officer) any of the following, and if **YES**, to any, please explain:

**SUMMARY COURT-MARTIAL** ☐ **YES** ☐ **NO** \_\_\_\_\_

**SPECIAL COURT-MARTIAL** ☐ **YES** ☐ **NO** \_\_\_\_\_

**ARTICLE 32 INVESTIGATION** ☐ **YES** ☐ **NO** \_\_\_\_\_

**GENERAL COURT-MARTIAL** ☐ **YES** ☐ **NO** \_\_\_\_\_

109. Have you ever imposed non-judicial punishment under U.C.M.J., Article 15? ☐ **YES** ☐ **NO**  
If **YES**, please explain: \_\_\_\_\_

#### COURT EXPERIENCE & JURY/MEMBER SERVICE

110. Have you ever watched any criminal trial (civilian or military) in person? ☐ **YES** ☐ **NO** If **YES**, please explain circumstances: \_\_\_\_\_

111. Have you or any family members or friends ever worked in the justice system (military or civilian)? ☐ **YES** ☐ **NO** If **YES**, please tell us who, when, what were their duties and are they still working there? \_\_\_\_\_

112. Have you or any family members or friends ever been a party to, a witness for any criminal trial (military or civilian)? ☐ **YES** ☐ **NO** If **YES**, who, when and what were the circumstances? \_\_\_\_\_

113. Have you served as a panel member in a courts-martial or a juror in any civilian criminal trial? ☐ **YES** ☐ **NO** If **YES**, please explain the type of case, whether provide the following information for each:

DATE	TYPE/NATURE OF CASE	FINDINGS?	PUNISHMENT ASSESSED?	WHAT WAS THE PUNISHMENT?
		<input type="checkbox"/> <b>NG</b> <input type="checkbox"/> <b>G</b>	<input type="checkbox"/> <b>YES</b> <input type="checkbox"/> <b>NO</b>	
		<input type="checkbox"/> <b>NG</b> <input type="checkbox"/> <b>G</b>	<input type="checkbox"/> <b>YES</b> <input type="checkbox"/> <b>NO</b>	
		<input type="checkbox"/> <b>NG</b> <input type="checkbox"/> <b>G</b>	<input type="checkbox"/> <b>YES</b> <input type="checkbox"/> <b>NO</b>	
		<input type="checkbox"/> <b>NG</b> <input type="checkbox"/> <b>G</b>	<input type="checkbox"/> <b>YES</b> <input type="checkbox"/> <b>NO</b>	
		<input type="checkbox"/> <b>NG</b> <input type="checkbox"/> <b>G</b>	<input type="checkbox"/> <b>YES</b> <input type="checkbox"/> <b>NO</b>	

#### LEGAL

114. Have you or anyone you know ever worked for a lawyer or law firm? ☐ **YES** ☐ **NO** If **YES**, who, which lawyer or law firm, what type of law does that lawyer/firm practice and what were your/their job responsibilities: \_\_\_\_\_



115. Do you know any lawyers, prosecutors or judges on a personal or professional basis?  
☐ **Yes** ☐ **No** If **YES**, who do you know, what type of law does that person practice and what is the nature of your relationship? \_\_\_\_\_

116. What is the first thing that comes to your mind when you think of a:

Criminal Defense Attorney: \_\_\_\_\_

Prosecuting Attorney: \_\_\_\_\_

#### CASE SPECIFICS

117. What criminal cases have you followed in the media and why did you follow those cases? \_\_\_\_\_

118. What is your opinion about the accuracy of media reports about crimes, in general? \_\_\_\_\_

119. This case involves the disclosure of classified information to WikiLeaks. The individual accused of committing this act is PFC Bradley Manning. Do you know, or believe you know, anything about this case, from any source, including the newspaper, radio, television or discussions with others? ☐ **Yes** ☐ **No** If **YES**, from which sources, what have you heard, read, seen or talked about concerning this case and what is your reaction to that information? \_\_\_\_\_

120. Based on what you have heard, read, seen or discussed concerning this case, what opinions have you formed concerning the people involved? \_\_\_\_\_

121. Based on what you have heard, read, seen or discussed concerning this case, have you formed any opinions on how the case is being handled and what the outcome should be?

---

---

---

---

---

---

---

---

---

---

**BEING GAY IN THE MILITARY**

122. Have you ever counseled a Soldier regarding his/her sexual preference? ☐ **Yes** ☐ **No** If **YES**, please explain what prompted your counseling of the soldier: \_\_\_\_\_

---

---

---

123. Have you ever initiated UCMJ action against a Soldier based on his/her sexual preference? ☐ **Yes** ☐ **No** If **YES**, please explain what prompted you to initiate UCMJ action: \_\_\_\_\_

---

---

---

124. Have you ever initiated administrative separation action against a Soldier based on his/her sexual preference? ☐ **Yes** ☐ **No** If **YES**, please explain what prompted you to initiate administrative separation action: \_\_\_\_\_

---

---

125. Have you ever recommended separation of a Soldier based on his her sexual preference? ☐ **Yes** ☐ **No** If **YES**, approximately how many times? \_\_\_\_\_

126. Do you agree with the repeal of DADT? Why or why not?

127. Have you seen any negative impact from the repeal of DADT? If so, what?

128. Have you seen any positive impact from the repeal of DADT? If so, what?

129. Are any members of your immediate family gay? ☐ YES ☐ NO

130. Are any of your close friends gay? ☐ YES ☐ NO

131. Do you oppose gay marriage? ☐ YES ☐ NO If YES, please explain why, \_\_\_\_\_

**GENDER IDENTITY DISORDER**

**Gender Identity Disorder is a diagnosis used by medical professionals to describe individuals who are discontent with the gender they were assigned at birth. Criteria for a diagnosis of GID include long-standing and strong identification with another gender, long-standing disquiet about the sex assigned or a sense of incongruity in the gender-assigned role of that sex and significant clinical discomfort or impairment at work, social situations, or other important life areas.**

132. Do you agree that an individual who is discontent with his/her gender has a disorder? ☐ **Yes**  
☐ **No** please explain why, \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
133. Do any members of your family have GID? ☐ **Yes** ☐ **No**
134. Do any of your close friends have GID? ☐ **Yes** ☐ **No**
135. What do you think when you see a cross-dresser on the street? \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
136. Do you agree that the military, under the former policy of DADT, would limit a Soldier's ability to fully explore his/her sexuality? ☐ **Yes** ☐ **No** please explain why \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
137. Are you open to the idea that a person with GID might struggle emotionally in a military environment? ☐ **Yes** ☐ **No** please explain why \_\_\_\_\_

**DEPLOYMENTS**

138. Have you deployed to Iraq or Afghanistan? ☐ YES ☐ NO If No, please skip to Question

141. If YES, please provide the date(s) and location(s) of your deployment: \_\_\_\_\_

139. How would you characterize your deployment experience? \_\_\_\_\_

140. Do you feel like your efforts contributed to the overall mission accomplishment? ☐ YES

☐ NO Please explain: \_\_\_\_\_

141. Did you work with Depart of State personnel during your deployment? ☐ YES ☐ NO If

Yes, what was your attitude towards DoS personnel? \_\_\_\_\_

**PUNISHMENT**

**IN A GENERAL COURT MARTIAL, MEMBERS MUST DETERMINE IF THE PROSECUTION HAS PROVED ITS CASE AGAINST THE DEFENDANT. IF THE MEMBERS FIND THE DEFENDANT NOT GUILTY, THE MEMBERS WILL NOT NEED TO CONSIDER PUNISHMENT. HOWEVER, IF THE PROSECUTION PROVES ITS CASE AGAINST THE DEFENDANT, THE MEMBERS MUST CONSIDER PUNISHMENT. SINCE THERE HAS BEEN NO EVIDENCE PRESENTED YET, THE COURT CANNOT KNOW WHAT THE EVIDENCE IN THIS CASE WILL BE, WHETHER OR NOT YOU WILL FIND THE DEFENDANT GUILTY OF ANYTHING AT ALL, AND IF THE MEMBERS WILL CONSIDER PUNISHMENT OR NOT.**

**THEREFORE, THE COURT MUST ASK QUESTIONS ABOUT YOUR THOUGHTS, FEELINGS AND OPINIONS ABOUT ALL APPLICABLE PUNISHMENT OPTIONS NOW, BEFORE YOU HAVE HEARD ANY EVIDENCE. THE FACT THAT THESE QUESTIONS ARE BEING ASKED OF YOU NOW IS NOT MEANT TO SUGGEST THAT**

YOU WILL EVER HAVE TO CONSIDER PUNISHMENT AND YOU SHOULD NOT ASSUME FROM ANY OF THESE QUESTIONS THAT THE DEFENDANT IS GUILTY. THE MEMBERS WILL ONLY CONSIDER PUNISHMENT IF THE PROSECUTION PROVES ITS CASE AGAINST THE DEFENDANT BEYOND A REASONABLE DOUBT.

142. Please rank in order of importance to you the following purposes for punishment in a criminal case (**1 being most important and 5 being least important**):

☐ CLOSURE    ☐ DETERRENCE    ☐ PUNISHMENT    ☐ REHABILITATION    ☐ REVENGE

PLEASE EXPLAIN YOUR ANSWER: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

FOR EACH OF THE FOLLOWING STATEMENTS, PLEASE INDICATE YOUR LEVEL OF AGREEMENT OR DISAGREEMENT AND EXPLAIN YOUR ANSWER:

143. No matter how noble the accused's goal was in committing the crime, this should have little impact on the appropriate punishment.

☐ STRONGLY AGREE    ☐ MODERATELY AGREE    ☐ SLIGHTLY AGREE  
☐ STRONGLY DISAGREE    ☐ MODERATELY DISAGREE    ☐ SLIGHTLY DISAGREE

PLEASE EXPLAIN YOUR ANSWER: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

144. If the case is a high profile case, it is important to ensure the punishment is severe to send the appropriate message.

☐ STRONGLY AGREE    ☐ MODERATELY AGREE    ☐ SLIGHTLY AGREE  
☐ STRONGLY DISAGREE    ☐ MODERATELY DISAGREE    ☐ SLIGHTLY DISAGREE

PLEASE EXPLAIN YOUR ANSWER: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

145. A person who has given classified information to an unauthorized person should receive a harsh sentence in order to deter others from committing a similar offense.

☐ STRONGLY AGREE    ☐ MODERATELY AGREE    ☐ SLIGHTLY AGREE  
☐ STRONGLY DISAGREE    ☐ MODERATELY DISAGREE    ☐ SLIGHTLY DISAGREE

PLEASE EXPLAIN YOUR ANSWER: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

146. It is possible that a criminal act can actually provide a benefit to an individual or a group of people.

☐ **STRONGLY AGREE**    ☐ **MODERATELY AGREE**    ☐ **SLIGHTLY AGREE**  
☐ **STRONGLY DISAGREE**    ☐ **MODERATELY DISAGREE**    ☐ **SLIGHTLY DISAGREE**

**PLEASE EXPLAIN YOUR ANSWER:** \_\_\_\_\_

---

---

---

147. A person who has given classified information to an unauthorized person should receive a harsh sentence in order to deter others from committing a similar offense.

☐ **STRONGLY AGREE**    ☐ **MODERATELY AGREE**    ☐ **SLIGHTLY AGREE**  
☐ **STRONGLY DISAGREE**    ☐ **MODERATELY DISAGREE**    ☐ **SLIGHTLY DISAGREE**

**PLEASE EXPLAIN YOUR ANSWER:** \_\_\_\_\_

---

---

---

148. As a result of your having been asked to fill out this questionnaire, have you formed any opinions about this case? ☐ **YES** ☐ **NO** If **YES**, please explain: \_\_\_\_\_

---

---

---

149. Knowing what only you can know about yourself, if you or someone you love was on trial for the charged offenses in this case, would you want someone with the same thoughts, feelings, opinions, attitudes and life experiences as you to serve as a Member? ☐ **YES** ☐ **NO** **PLEASE EXPLAIN YOUR ANSWER:** \_\_\_\_\_

---

---

---

150. Is there anything that was not asked that you believe is important to know about you? ☐ **YES** ☐ **NO** If **YES**, please explain: \_\_\_\_\_

---

---

---

151. Is there anything that you would like to discuss privately with the court? ☐ **YES** ☐ **NO** If **YES**, please explain: \_\_\_\_\_

---

---

---

$\mathbf{y}_i$ 

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**Prosecution Notice to Court of  
Identification of  
Additional CIA Information**

12 July 2012

## NOTICE

The United States hereby provides notice to the Court that the United States learned on 11 July 2012 that the CIA has drafted another report analyzing the impact of the WikiLeaks disclosures on a discrete matter. The report is a follow-on report to the original WikiLeaks Task Force Report. The United States intends to review the additional report on 13 July 2012 and intends to submit any applicable filings to the Court no later than 3 August 2012.

a

ASHDEN FEIN  
MAJ, JA  
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 12 July 2012.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel



**v.**

**Prosecution Request for Leave  
until 18 July 2012 to File  
a Protective Order and Motion for  
Interim Protective Order  
to Preclude Defense from Publishing  
Defense Notice under MRE 505(h)(3):  
Charged Documents**

1. The United States requests leave of the Court until 18 July 2012 to file a Motion for a protective order in accordance with the Court's Interim Order: Government Request for Leave to File Protective Order(s) dated 28 March 2012 and the Court's Order: Government Motion: Protective Order(s) dated 24 April 2012.

2. The United States also requests that the Court order the Defense not to publish Defense Notice under Military Rule of Evidence 505(h)(3): Charged Documents (hereinafter Defense Notice) until the United States has the ability to determine whether a request for a protective order is necessary.

3. The United States believes that the Defense Notice may contain classified information. In general, the Defense describes the content of a classified video, for which an original classification authority (OCA) conducted a classification review and identified as classified. The United States is working with CENTCOM, the relevant OCA, to determine whether the information the Defense provided is classified because it came from a classified video. To the best of the prosecution's knowledge, the information provided by the Defense is only available to an individual who has viewed the classified video. CENTCOM advised the prosecution that it requires additional time to make this determination because the subject matter expert for this topic has departed the command. Accordingly, the United States requests until 18 July 2012 to coordinate with CENTCOM and to file a Protective Order, if necessary.

4. This request will not necessitate any delay in the proceedings or delay in responding to the defense, as the United States still intends to respond on 11 July 2012 to the Defense Notice in a separate filing.



ALEXANDER VON ELTEN  
CPT, JA  
Assistant Trial Counsel

## David Coombs

**From:** David Coombs <coombs@armycourtartialdefense.com>  
**Sent:** Monday, July 16, 2012 7:49 PM  
**To:** 'Lind, Denise R COL USARMY (US)'; 'Williams, Patricia A CIV (US)'; 'Jefferson, Dashawn MSG USARMY (US)'  
**Cc:** Hurley, Thomas F MAJ OSD OMC Defense; 'Tooman, Joshua J CPT USARMY (US)'; 'Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA'; 'Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA'; 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; 'Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA'; Alexander.VonElten@jfhqncr.northcom.mil  
**Subject:** United States v. Martinelli Question  
**Attachments:** Martinelli.docx

Ma'am,

I've had an opportunity to look at the *United States v. Martinelli* case that you asked me about today in oral argument, and do not believe that it can be read to support the proposition that the Government is entitled to a lesser-included offense for a fatally defective specification. First, as I indicated in oral argument today, the context in which *Martinelli* was decided is very different than the context in which the issue presents itself here. In *Martinelli*, the court was assessing the providence of the accused's guilty plea after a case was decided; it was not assessing whether the government was entitled to an instruction on a lesser-included offense at the outset of the case where the court has found as a fact that the evidence falls short of establishing a legally cognizable defense.

More importantly, though, the reason *why* the offense was not cognizable in *Martinelli* is very different than the reason why it is not cognizable here. This difference means that an instruction on the lesser included offense might have been appropriate in *Martinelli*, but not in the instant case. In *Martinelli*, the accused was charged under clause 3 with violating the Child Pornography Prevention Act (CPPA) for certain acts he was alleged to have committed while in Germany. After the accused pled guilty to the specifications, the court determined that the CPPA could not apply extraterritorially to the conduct at issue; hence, the clause 3 offenses were not cognizable. The court upheld clause 1 and 2 offenses as being lesser-included offenses of the clause 3 offense.

However, it is important to look at the specifications in *Martinelli* to understand why they could survive in that case and why they cannot survive in the instant case. The specifications in *Martinelli* were as follows:

Specification 1: knowingly mailing, transporting or shipping child pornography in interstate or foreign commerce (by computer) in violation of § 2252A(a)(1) (specifically, sending images over the Internet from the Network Internet Café in Darmstadt, Germany);

Specification 2: knowingly receiving child pornography that has been mailed, shipped or transported in interstate or foreign commerce (by computer) in violation of § 2252A(a)(2)(A) (specifically, downloading images from the Internet in the Network Internet Café in Darmstadt, Germany);

Specification 3: knowingly reproducing child pornography for distribution through the mails, or in interstate or foreign commerce (by computer) in violation of § 2252A(a)(3) (specifically, downloading images from the Internet; copying them to hard drive and transmitting the copied files to approximately twenty individuals over the Internet in the Network Internet Café in Darmstadt, Germany);

Specification 4: knowingly possessing child pornography on land and in a building used by and under

APPELLATE EXHIBIT CCX  
PAGE REFERENCED:  
PAGE 1 OF 2 PAGES

the control of the United States Government in violation of § 2252A(5)(A) (specifically, possessing approximately fifty diskettes containing child pornography in buildings at the Cambrai Fritsch Kaserne).

Notably, once the judge removed the reference to “in violation of [the CPPA],” the underlying factual acts could still be proved so as to form the basis for an Article 134 offense. In other words, in *Martinelli*, it wasn’t the Government’s underlying theory that was deficient. It was simply that the statute did not extend so as to cover acts outside the continental United States.

Otherwise stated, even though the offenses were not cognizable as crimes under the CPPA, the *factual acts* underlying the original specifications could still be proven and made the basis for a lesser-included offense under Article 134. For instance, under specification 1, the government was still capable of proving that the accused “knowingly mailing, transporting or shipping child pornography in interstate or foreign commerce (by computer)” and that such conduct was prejudicial to good order and discipline. Removal of the offending statute (the CPPA) from the specification did not change the ability of the government to prove the underlying offense.

In the instant case, the factual acts underlying the original specification cannot be proven because the conduct involves “exceeding authorized access” *as defined by* section 1030. In other words, the specification cannot be proved simply by removing reference to section 1030 as the court did in *Martinelli* and other cases like it. See *United States v. Monette*, 2006 WL 6625267, \*1 (Army Ct. Crim. App.) (“Our court modified the findings of guilty to Specifications 8, 9, 11, 12, and 13 of Additional Charge II by *deleting all Title 18 nomenclature referring to the CPPA*, and, for each affected specification, affirmed a lesser-included simple disorder under Article 134”) (emphasis supplied).

For instance, in specification 13 of Charge II, the Government pleads that PFC Manning:

did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, having knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer, and by means of such conduct having obtained . . . more than seventy-five classified United States Department of State cables, willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1)[.]

If the Court were simply to remove the language “in violation of 18 U.S. Code Section 1030(a)(1)” from the specification as did the court in *Martinelli*, the Government would still not be able to prove the offense because the offense derives from section 1030 and “exceeds authorized access” is defined by the terms of that statute. Thus, this court cannot simply create a lesser-included offense by deleting the Section 1030 “nomenclature” from the specification as the court did in *Martinelli*.

In order to state an Article 134 offense based on this conduct, the Government would actually need to *change* the specification to allege some other conduct not in the specification (e.g. the accused used Wget to obtain the cables). In other words, we would be dealing with an amendment to the specification and not a lesser-included offense. The Defense submits that this would be a major amendment under R.C.M. 603 that cannot be made over the objection of the accused.

To the Defense’s knowledge, there is no military case that has permitted the government to proceed with lesser-included offense of a clause 3 offense which is not legally cognizable because the Government does not have the factual evidence to proceed. Specifically, there is no case (*Martinelli* included) where a court has determined pretrial that the Government doesn’t have any evidence for an essential element of an offense and nevertheless has allowed the government to go forward with an unchanged lesser-included offense.

- Accordingly, the Defense submits that *Martinelli* does not permit this Court to find a lesser-included offense where the entire theory underlying the specification is deficient. Any Article 134 offense would require a major amendment to the specification which is not permitted over the objection of the accused.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)  
[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com)

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**Disputed Questions**

**in Proposed  
Court Member Questionnaires**

**17 July 2012**

A. The prosecution objects to the inclusion of the following defense-proposed questions and statements in the supplemental court member questionnaire:

1. Do you now have, or have you ever had the authority to train, supervise, assign, evaluate, or discipline others? ☐ YES ☐ NO IF YES, Please describe your feelings concerning the importance of mentoring junior enlisted:

2. Why do junior enlisted need to be mentored?

3. Have any of you ever heard the expression "with proper leadership, failure is not an option?" If so, what does that term mean to you?

4. Do you believe that the command should revoke a soldier's security clearance if the soldier exhibits any signs of mental or emotional instability?  
☐ YES ☐ NO If YES, please indicate why:

5. Do you believe that the command should revoke a soldier's security clearance if the soldier exhibits any signs aggression towards other soldiers?  
☐ YES ☐ NO If YES, please indicate why:

6. Do you believe that a command should deploy a soldier if the soldier exhibits signs of mental or emotional instability?  
☐ YES ☐ NO If NO, please indicate why:

7. Please list the civil clubs, societies, professional associations, or other organizations to which you now belong, or to which you have belonged in the past:

8. Have you ever served as an officer or held a position of leadership in any of these organizations?  
☐ YES ☐ NO If YES, please explain

9. To which charitable organizations do you contribute money, time, services or resources, and why did you choose those organizations?

10. What are your hobbies:

11. What do you enjoy doing in your spare time:

APPELLATE EXHIBIT CCXI  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

12. What were the last three books you have read:
13. In general, what types of books do you most often read?
14. Have you ever read a book about releasing classified information or any similar action?  
☐ YES ☐ NO If YES, which book, who was the author, what trial or crime and why were you interested?
15. Have you ever written a letter to the editor? ☐ YES ☐ NO If YES, about what issue did you write and why did you decide to write the letter:
16. Do you usually read for ☐ ENTERTAINMENT PURPOSES or for ☐ BUSINESS PURPOSES?
17. Approximately how many hours per week do you spend watching television?
18. What television shows do you watch regularly:
19. How often do you go to see a movie?
20. In general, what types of movies do you most prefer (i.e. romantic comedies, dramas, action, mysteries, science fiction, etc.)?
21. What are the last three movies you went to see:
22. Please list the 3 people you admire or respect *the most* and tell us *why*:
23. Please list the 3 people you admire or respect *the least* and tell us *why*:
24. Please list the one *person* you feel most influenced your life, either positively or negatively, and tell us *why*:
25. Please list the one *event* you feel most influenced your life, either positively or negatively, and tell us *why*:
26. Does anyone believe that young individuals are susceptible to make mistakes in judgment?  
☐ YES ☐ NO Please indicate why you feel this way.
27. Does anyone believe that the legal drinking age should be lower than 21 years of age?  
☐ YES ☐ NO Please indicate why you feel this way.
28. Does anyone believe that 21 is too young for a person to get married? ☐ YES ☐ NO Please indicate why you feel this way.
29. Why do you believe that rental car companies do not rent cars to individuals under the age of 25?

30. Have you ever heard the expression "kids these days think that they know it all?"  
☐ YES ☐ NO If YES, what does this expression mean to you?
31. Do you believe that the typical 20 something-year-old believes that they "know it all?"  
☐ YES ☐ NO Please indicate why you feel this way.
32. Do believe that it is not unusual for a person in their early twenties to believe that they can do something to make a difference or change the world? ☐ YES ☐ NO Please indicate why you feel this way.
33. Have you ever signed a petition? ☐ YES ☐ NO If YES, please tell us what were the issue(s):
34. Have you ever participated in a march, protest or demonstration? ☐ YES ☐ NO If YES, please tell us when and what were the issue(s):
35. Have you ever known anyone who you believe suffered from severe emotional problems? ☐  
YES ☐ NO If YES, please explain:
36. Have you or any family members or any close friends ever undergone counseling, treatment, or hospitalization for psychiatric, emotional, family, or behavioral problems? ☐ YES ☐ NO If YES, please tell us who and provide the details, including the name of the hospital, doctor or counselor seen, diagnosis, treatment and outcome:
37. Have you followed any criminal cases that involved testimony about severe emotional problems experienced by the person accused of a crime? ☐ YES ☐ NO If YES, what was the case, why did you follow it, what was the outcome and what were your feelings about the outcome?
38. Have you or any family members or close friends ever volunteered time, money, services, materials, etc. to any children's protective service, crisis intervention, emergency response, emergency medical care, fire department, search and rescue, shelters, or any organizations involved in helping victims of abuse, in general? ☐ YES ☐ NO If YES, who was involved, how was that person involved and why did that person become involved?
39. Have you or any member of your family or friends ever used any of the above services?  
☐ YES ☐ NO If YES, please explain:
40. Do you know anyone who has experienced any type of abusive relationship (sexual abuse, physical abuse, verbal abuse, emotional/psychological abuse, etc.)? ☐ YES ☐ NO If YES, please explain:
41. If a person experiences abuses as a child, how do you believe that might impact their social abilities with others as a young adult?
42. Do you believe the military justice should be influenced by outside civilian pressures to send a message in certain cases? ☐ YES ☐ NO PLEASE EXPLAIN YOUR ANSWER:

43. Have you ever watched any criminal trial (civilian or military) in person? ☐ YES ☐ NO If YES, please explain circumstances:

44. Do you oppose gay marriage? ☐ YES ☐ NO If YES, please explain why

45. The following description given before a series of Gender Identity Disorder questions: **Gender Identity Disorder is a diagnosis used by medical professionals to describe individuals who are discontent with the gender they were assigned at birth. Criteria for a diagnosis of GID include long-standing and strong identification with another gender, long-standing disquiet about the sex assigned or a sense of incongruity in the gender-assigned role of that sex and significant clinical discomfort or impairment at work, social situations, or other important life areas.**

46. Do you agree that an individual who is discontent with his/her gender has a disorder?  
☐ YES ☐ NO please explain why

47. Do any members of your family have GID? ☐ YES ☐ NO

48. Do any of your close friends have GID? ☐ YES ☐ NO

49. Do you agree that the military, under the former policy of DADT, would limit a Soldier's ability to fully explore his/her sexuality? ☐ YES ☐ NO please explain why

50. Are you open to the idea that a person with GID might struggle emotionally in a military environment? ☐ YES ☐ NO please explain why

51. How would you characterize your deployment experience?

52. Do you feel like your efforts contributed to the overall mission accomplishment?  
☐ YES ☐ NO Please explain:

53. The following description given before a series of punishment questions: **IN A GENERAL COURT MARTIAL, MEMBERS MUST DETERMINE IF THE PROSECUTION HAS PROVED ITS CASE AGAINST THE DEFENDANT. IF THE MEMBERS FIND THE DEFENDANT NOT GUILTY, THE MEMBERS WILL NOT NEED TO CONSIDER PUNISHMENT. HOWEVER, IF THE PROSECUTION PROVES ITS CASE AGAINST THE DEFENDANT, THE MEMBERS MUST CONSIDER PUNISHMENT. SINCE THERE HAS BEEN NO EVIDENCE PRESENTED YET, THE COURT CANNOT KNOW WHAT THE EVIDENCE IN THIS CASE WILL BE, WHETHER OR NOT YOU WILL FIND THE DEFENDANT GUILTY OF ANYTHING AT ALL, AND IF THE MEMBERS WILL CONSIDER PUNISHMENT OR NOT. THEREFORE, THE COURT MUST ASK QUESTIONS ABOUT YOUR THOUGHTS, FEELINGS AND OPINIONS ABOUT ALL APPLICABLE PUNISHMENT OPTIONS NOW, BEFORE YOU HAVE HEARD ANY EVIDENCE. THE FACT THAT THESE QUESTIONS ARE BEING ASKED OF YOU NOW IS NOT MEANT TO SUGGEST THAT YOU WILL EVER HAVE TO CONSIDER PUNISHMENT AND YOU SHOULD NOT ASSUME FROM ANY OF THESE QUESTIONS THAT THE DEFENDANT IS GUILTY. THE MEMBERS WILL ONLY CONSIDER PUNISHMENT IF THE PROSECUTION PROVES ITS CASE AGAINST THE DEFENDANT BEYOND A REASONABLE DOUBT.**



54. Knowing what only you can know about yourself, if you or someone you love was on trial for the charged offenses in this case, would you want someone with the same thoughts, feelings, opinions, attitudes and life experiences as you to serve as a Member? ☐ YES ☐ NO *PLEASE EXPLAIN YOUR ANSWER:*

B. The prosecution and the defense disagree on the wording of the below questions. The defense proposed question is listed with "a" and the prosecution proposed question is listed with "b."

1a. This case involves the disclosure of classified information to WikiLeaks. The individual accused of committing this act is PFC Bradley Manning. Do you know, or believe you know, anything about this case, from any source, including the newspaper, radio, television or discussions with others? ☐ YES ☐ NO If YES, from which sources, what have you heard, read, seen or talked about concerning this case and what is your reaction to that information? *PLEASE EXPLAIN YOUR ANSWER:*

1b. The Accused in this case is PFC Bradley Manning. The website WikiLeaks is also involved in this case. Do you know, or believe you know, anything about this case, from any source, including the newspaper, radio, television, or discussions with others? ☐ YES ☐ NO If YES, from which sources, what have you heard, read, seen or talked about concerning this case and what is your reaction to that information?

2a. *FOR THE FOLLOWING STATEMENTS, PLEASE INDICATE YOUR LEVEL OF AGREEMENT OR DISAGREEMENT AND EXPLAIN YOUR ANSWER:* No matter how noble the accused's goal was in committing the crime, this should have little impact on the appropriate punishment.

☐ STRONGLY AGREE ☐ MODERATELY AGREE ☐ SLIGHTLY AGREE  
☐ STRONGLY DISAGREE ☐ MODERATELY DISAGREE ☐ SLIGHTLY DISAGREE

*PLEASE EXPLAIN YOUR ANSWER:*

2b. Do you believe that an Accused's motive in committing a crime is relevant to punishment? If yes, please explain your answer.

3a. *FOR THE FOLLOWING STATEMENTS, PLEASE INDICATE YOUR LEVEL OF AGREEMENT OR DISAGREEMENT AND EXPLAIN YOUR ANSWER:* A person who has given classified information to an unauthorized person should receive a harsh sentence in order to deter others from committing a similar offense.

☐ STRONGLY AGREE ☐ MODERATELY AGREE ☐ SLIGHTLY AGREE  
☐ STRONGLY DISAGREE ☐ MODERATELY DISAGREE ☐ SLIGHTLY DISAGREE

*PLEASE EXPLAIN YOUR ANSWER:*

3b. Do you believe that a person should receive a harsh sentence in order to deter others from committing a similar offense? If yes, please explain your answer.

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
HHC, U.S. Army Garrison  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

)  
) **ORDER:**  
) **GOVERNMENT MOTION:**  
) **PROTECTIVE ORDER(S)**  
) **ADDENDUM**  
)  
) **DATED: 17 July 2012**

1. This Order applies when the Defense proposes to release Defense Court filings or proposed filings publicly.
2. A pleading is "filed" with the Court when it is identified as an exhibit on the record at an Article 39(a) session. Pleadings served on the opposing party that have not been identified on the record at an Article 39(a) session are "proposed filings".
3. This Order is issued IAW MRE 505(g) and (h), MRE 506(g) and (h), RCM 701(g) and RCM 806(d), and *Seattle Times v. Rhinehart*, 104 S.Ct. 2199 (1984). The Order provides procedures for the Government to request protective order(s) prior to any public release of Defense Court filings or proposed filings. The Court finds this Order necessary under the above authorities. The Government has provided the Defense both classified information and government information subject to protective order under MRE 505(g)(1) and MRE 506(g). This Court has issued a protective order for classified information provided to the Defense in discovery. The Defense accepted such discovery and agreed to comply with the protective orders. There have been two classified information spillage incidents to date in this case.
4. This Order supplements the Court Order: Government Motion: Protective Order(s) issued on 24 April 2012.

**ORDER:**

1. The Defense will notify the Government of each Defense Court filing or proposed filing intended for public release. Defense will provide the Government with the original filing and the redacted filing intended for public release.
2. Government motions for protective order will:
  - a. address each Defense Court filing or proposed Court filing individually and identify, with particularity, each portion of the filing to which the Government objects to public release and the legal basis for each objection to public release.

APPELLATE EXHIBIT \_\_\_\_\_  
PAGE REFERENCED: \_\_\_\_\_  
PAGE 1 OF 2 PAGES

(212)

b. provide proposed findings of fact for the Court with respect to each portion of each filing to which the Government objects to public release.

3. Suspend Dates for Defense Court filings and proposed filings the Defense intends to publicly release. The Court is currently scheduling Article 39(a) sessions with the following schedule: 2 weeks to file motions; 2 weeks to file responses; 5 days to file replies.

a. NLT the **scheduled filing date for motions, responses, or reply** for each Article 39(a) session, the Defense shall provide the Government notice IAW paragraph (1) of this Order.

b. The Government shall provide the notice to the Court if it does not intend to object, or whether it requires coordination for a specific filing, **NLT 5 duty days after the Defense filing.**

c. If the Government provides notice to the Court that it requires additional time to conduct further review IAW paragraph (3)(b) of this Order, the Government shall provide the Court with information ordered in paragraph (2) of this Order **NLT 10 duty days after providing notice** IAW paragraph (3)(b) to the Court.

The Court will grant motions for continuance for good cause.

4. The Defense will not publicly release any Defense Appellate Exhibit or proposed filing with the Court to which the Government objects until after the Government motion(s) for protective order are addressed at the next scheduled Article 39(a) session.

5. The Defense will not disclose any information known or believed to be subject to a claim of privilege under MRE 505 or MRE 506 without specific Court authorization. Prior to any disclosure of classified information, the Defense will provide notice under MRE 505(h) and follow the procedures under that rule.

6. Personal identifying information (PII) will be redacted from all Defense filings publicly released. PII includes personal addresses, telephone numbers, email addresses, first 5 digits of social security numbers, dates of birth, financial account numbers, and the names of minors.

7. To protect the safety of potential witnesses all persons who are not parties to the trial shall be referenced by initials of first and last name in any Defense filing publicly released. The Defense will redact job positions and titles held only by one individual.

So **ORDERED**: this 17th day of July 2012.



DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

## UNITED STATES

 $\mathbf{y}_i$ 

**MANNING, Bradley E., PFC**  
U.S. Army, [REDACTED]  
Headquarters and Headquarters Company, U.S.  
Army Garrison, Joint Base Myer-Henderson Hall,  
Fort Myer, VA 22211

### ADDITIONAL RESEARCH REQUEST BY THE COURT: VALUATION

DATED: 17 July 2012

1. The Court requested the Defense to obtain authority for its argument that the Government would have to establish proof of a thieves' market in order to use such a method to establish value under Section 641.
2. The Defense respectfully requests the Court to consider the following authority.

3. The statute at issue provides that:

“Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

“Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted-- “Shall be fined under this title or imprisoned not more than ten years, or both; but if the value of such property in the aggregate, combining amounts from all the counts for which the defendant is convicted in a single case, does not exceed the sum of \$1,000, he shall be fined under this title or imprisoned not more than one year, or both.” 18 U.S.C. § 641.<sup>1</sup>

<sup>1</sup> Section 641 was amended in 1996 by striking the value of “\$100” and replacing it with the value of “\$1,000.” Oct. 11, 1996, Pub.L. 104-294, Title VI, Section 606(a), 110 Stat. 3511. Many of the cases cited herein involved prosecutions under the pre-1996 § 641, where the value necessary for a felony offense was only \$100.

4. Section 641 additionally defines the term “value” to mean “face, par, or market value, or cost price, either wholesale or retail, whichever is greater.” *Id.*

5. The Government must proffer some evidence of the property’s actual value; the panel members are not permitted to infer the requisite value simply from the nature of the property at issue. See *United States v. DiGilio*, 538 F.2d 972, 980-81 (3d Cir. 1976); *United States v. Horning*, 409 F.2d 424, 426 (4th Cir. 1969); *United States v. Wilson*, 284 F.2d 407, 408 (4th Cir. 1960). *Wilson* provides the clearest demonstration of this proposition. In that case, the defendant was charged with the theft of 72 rifles at a time when Section 641 only required the property to have a value of \$100 or more to support a felony conviction. *Id.* at 408. The government offered no evidence of the value of the rifles, but the jury found the defendant guilty on the felony charge. See *id.*<sup>2</sup> The Fourth Circuit vacated the defendant’s conviction because no evidence of actual value was offered by the government, stating that:

“[w]e are asked to take judicial notice that 72 rifles are worth more than \$100.00, but we cannot on the basis of anything in the testimony form a judgment as to value for the purpose of supporting the greater penalty. Nor, in the absence of any proof of value, could the jury be permitted to speculate on this point merely from the appearance of the articles. A fact which distinguishes a violation punishable by imprisonment for not more than one year from a violation punishable by imprisonment for ten years cannot be permitted to rest upon conjecture or surmise.” *Id.*

6. Similarly, in reducing the defendant’s conviction from a felony to a misdemeanor, the *DiGilio* court explained that “[p]ermitting juror speculation as to value in the absence of evidence was, for the reasons set forth in *United States v. Wilson* and the cases which have followed it, error.” 538 F.2d at 981. At the very least, the Government must provide a sufficient foundation “to enable the jury to find beyond a reasonable doubt this essential element of the felony charged.” *Horning*, 409 F.2d at 426.

7. As noted above, Section 641 defines the term “value” to mean “face, par, or market value, or cost price, either wholesale or retail, whichever is greater.” 18 U.S.C. Section 641 (emphasis added). The most common method used to prove value of stolen or converted property under § 641 is proof of market value of some sort. In this context, market value has been defined as “the price at which the minds of a willing buyer and a willing seller would meet.” *Digilio*, 538 F.2d at 979. Often, the resale price of the goods can be strong evidence of the market price. See, e.g. *United States v. Robie*, 166 F.3d 444, 451 (2d Cir. 1999); *United States v. Morison*, 604 F.Supp. 655, 664-65 (D. Md. 1985).

8. However, there need not be a legitimate, open market for the property in question for it to have a readily ascertainable “market value” under Section 641. As explained by then-Judge

---

<sup>2</sup> It should be noted that the jury needed only to conclude that each rifle had a value of at least \$1.39 in order to find that the requisite \$100 value was satisfied here. See *DiGilio*, 538 F.2d at 980-81 (discussing the *Wilson* case). Even discounting for the fact that *Wilson* was decided in 1960, it is highly unlikely that the jury’s speculation as to the value of the rifles was too high.

Blackmun in *Churder*, “the value measure contemplated by 641 is [not] restricted to an open market price ‘between honest, competent and disinterested men’. We apply to the statute what we feel is its obvious, and certainly its practical, meaning, namely, the amount the goods may bring to the thief.” *Churder v. United States*, 387 F.2d 825, 832-33 (8th Cir. 1968) (Blackmun, J.). Like the *Churder* court, several courts of appeals recognize that market value may be proved under § 641 by reference to a “thieves’ market.” See *United States v. Sargent*, 504 F.3d 767, 771 (9th Cir. 2007); *Robie*, 166 F.3d at 449; *United States v. Oberhardt*, 887 F.2d 790, 792 (7th Cir. 1989) (“[i]t is evident from the last paragraph of § 641 that Congress sanctioned a number of different methods of valuation for the purposes of determining whether a violation should be classified and sentenced as a misdemeanor or as a felony.”)

9. It is well settled that the valuation of stolen goods according to the concept of a “thieves’ market” is an appropriate method for determining the “market value” of goods for the purposes of § 641.”); *Jeter*, 775 F.2d at 680; *United States v. Gordon*, 638 F.2d 886, 889 (5th Cir. 1981) (“[t]he marijuana was an illegal substance, and the Government paid for its destruction. On those facts, Gordon says the marijuana was not a “thing of value,” insisting that the required “value” must be value to the Government, not to smugglers or outlaws. We disagree . . . ‘Value’ may also be ‘thieves value.’”); *DiGilio*, 538 F.2d at 979; see also *Morison*, 604 F.Supp. at 664-65. Similar to the determination of regular market value, the actual or attempted resale price can be strong evidence of the thieves’ market value. See *United States v. Jeter*, 775 F.2d 670, 680 (6th Cir. 1985); *Morison*, 604 F.Supp. at 664-65.

10. However, proof of the existence of a thieves’ market is insufficient to satisfy the government’s burden of proof as to the value of the property. *DiGilio*, 538 F.2d at 979. The *DiGilio* court explained that if “there is no proof regarding exchange price in the thieves’ market generally, evidence showing only the existence of that market is insufficient on the question of value for felony sentences under § 641.” *Id.* In addition to proving the existence of a thieves’ market for particular property, the Government must offer some evidence of the value of that property on that thieves’ market; in the absence of such evidence, a jury’s finding of the requisite value under § 641 would be pure speculation. See *DiGilio*, 538 F.2d at 981; see also *Horning*, 409 F.2d at 426 (holding that juror speculation as to value of property is impermissible); *Wilson*, 284 F.2d at 408 (same). For these reasons, the *DiGilio* court vacated *DiGilio*’s felony conviction:

“We do not approve the [trial] court’s charge that the jury could determine the cost of gathering and producing the information or the market value in a thieves’ market ‘on the basis of (its) common knowledge and experience, and the reasonable inferences to be drawn from the evidence.’ No reasonable inferences of market value of property involved in any particular theft could be drawn from the evidence.” 538 F.2d at 981.

11. In the instant case, the Defense is unaware of any allegation that PFC Manning sold or attempted to sell the database he is alleged to have converted. Absent evidence of a sale or an attempted sale by PFC Manning or evidence of a thieves’ market, such a valuation option is not available to the Government.

CONCLUSION

12. For the reasons articulated above, the Defense requests this Court deny the Government's request to instruction on "thieves market" absent proof which satisfies the above requirements.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'DE COOMBS', with a long horizontal flourish extending to the right.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, [REDACTED]  
Headquarters and Headquarters Company, U.S.  
Army Garrison, Joint Base Myer-Henderson Hall,  
Fort Myer, VA 22211

ADDITIONAL RESEARCH  
REQUEST BY THE COURT:  
CONVERSION

DATED: 17 July 2012

1. The Court requested the Defense to obtain authority for its argument that the Government is required to demonstrate a serious or substantial interference with the Government's right to use and control its property.
2. The Defense respectfully requests the Court to consider the following authority.

ARGUMENT

3. It is well-settled that the Government must prove that the accused's actions resulted in a substantial or serious interference with the Government's ownership rights in its property in order to secure a Section 641 conviction for knowing conversion. In *United States v. Collins*, 56 F.3d 1416 (D.C. Cir. 1995) (per curiam), the court explained that "[t]he cornerstone of conversion is the unauthorized exercise of control over property in such a manner that *serious interference* with ownership rights occurs." 56 F.3d at 1420 (emphasis in original).
4. *Collins* involved a Section 641 prosecution of a technical analyst at the Defense Intelligence Agency who used the agency's classified computer system to create and maintain hundreds of documents relating to the analyst's ballroom dance activities. *Id.* at 1418. In the Section 641 prosecution, the Government alleged that the defendant converted, among other things, the agency's computer time and storage space. *Id.* The court held that there was insufficient evidence to support the charge relating to conversion of computer time and storage because the Government did not prove that the defendant's use of the system for non-work related tasks seriously interfered with the Government's property rights in that system:

[T]he government did not provide a shred of evidence in the case at bar that [defendant] seriously interfered with the government's ownership rights in its computer system. While [defendant] concedes he typed in data and stored information on the computer regarding his personal activities, no evidence exists that such conduct prevented him or others from performing their official duties on the computer. The government did not even attempt to show that [defendant's]



use of the computer prevented agency personnel from accessing the computer or storing information. Thus, [defendant's] use of the government computer in no way seriously interfered with the government's ownership rights.

*Id.* at 1421.

5. Along similar lines, the Eighth Circuit in *United States v. May*, 625 F.2d 186 (1980), reversed the defendant's Section 641 conviction because the district court failed to instruct the jury that conversion under Section 641 required a finding that the defendant's conduct seriously violated the Government's property rights. 625 F.2d at 188. In *May*, the defendant, a former Adjutant General of the Iowa National Guard, "directed a series of unauthorized flights, using National Guard aircraft, fuel and personnel, that served his own convenience rather than that of the National Guard." *Id.* at 188-89. More specifically, the defendant directed 11 unauthorized flights that allowed him to visit his fiancé in various parts of the country. *Id.* at 189. In holding that the district court's failure to instruct the jury on the serious interference element of conversion was reversible error, the *May* Court explained that:

The touchstone of conversion is the exercise of such control over property that serious interference with the rights of the owner result, making it just that the actor pay the owner the full value of the object.

\* \* \*

The problem with the district court's instruction is that it assumes that any misuse or unauthorized use of property is a conversion.

\* \* \*

[T]he instruction misses the mark because it does not mention the requirement that the misuse constitute a serious violation of the owner's right to control the use of the property.

*Id.* at 192.

6. Similarly, the Ninth Circuit in *United States v. Kueneman* reversed the defendant's Section 641 conversion conviction because of an inadequate showing that the defendant's conduct seriously interfered with the Government's property rights. No. 94-10566, 1996 WL 473690, at \*2 (9th Cir. Aug. 20, 1996) (unpublished). In that case, the defendant was the president of a non-profit organization that participated in a Department of Housing and Urban Development's (HUD) program that leased HUD homes to non-profit organizations for \$1/year, provided that the non-profit organizations agreed to sublet these homes to homeless persons. *Id.* at \*1. The defendant's alleged conversion occurred when he allowed his daughter to live in one of the HUD homes for six weeks after quarrelling with her husband. *Id.* The Ninth Circuit determined that the Government's evidence of conversion was insufficient as a matter of law. *Id.* The court explained that "not all misuse of government property is conversion. To prove conversion, the government must show [defendant's] misuse of the HUD house was a 'serious interference with the [government's] property rights.' A 'serious interference' is one that prevents the government

from making some other use of the property.” *Id.* at \*1-2 (internal citations omitted). The evidence of conversion was thus held to be insufficient because “[t]he government offered no evidence that it had other contemporaneous uses for the HUD home.” *Id.* at \*2.

7. Finally, in *United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991), the Fourth Circuit affirmed a Section 641 conviction of a former Department of Defense employee who gave secret Department of Defense documents to his new employer (Boeing Aerospace Co.) and other defense contractors. 932 F.2d at 309. The defendant also converted some of the documents by incorporating secret information from them into his unclassified reports. *Id.* Though affirming his conviction, the court noted approvingly that the district court “recognized that ‘substantial interference with government property rights’ was an element of conversion [under Section 641]. [The district court] permitted the introduction of the contents of the documents mentioned in the conversion counts and properly instructed the jury on this issue.” *Id.* at 310.

8. Thus, it is settled law that the Government must show that PFC Manning’s alleged actions resulted in a substantial or serious interference with the Government’s ownership rights in the charged databases in order for PFC Manning to be found guilty of knowing conversion under Section 641.

#### CONCLUSION

9. Based upon the above authority, the Defense respectfully requests that the Court provide the Defense requested instruction on conversion.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)

16 June 2008- Drew pleaded not guilty.

23 July 2008- Drew filed three motions to dismiss the indictment on grounds of failure to state an offense, vagueness, and unconstitutional delegation of prosecutorial power.

1 August 2008- Electronic Frontier Foundation and the Cyberlaw Clinic at Harvard's Berkman Center for Internet & Society submitted an amicus brief supporting dismissal of the case

4 September 2008 - In a hearing, Judge George H. Wu denied Drew's motions to dismiss the indictment based on vagueness and improper delegation of authority, but kept her motion to dismiss for failure to state an offense under advisement.

26 November 2008 - The jury returned a verdict acquitting Drew on the felony CFAA charges and finding her guilty on misdemeanor CFAA charges. The jury deadlocked on the felony conspiracy count. Counsel for Drew (now including Professor Orin Kerr) indicated that they would file a motion for a new trial, and the court set a hearing for 29 December 2008. The court took the Drew's renewed motion for judgment of acquittal under submission.

15 December 2008 - Counsel for Drew filed a supplement to their motion for judgment of acquittal, requesting the Court to decide the issue that it had taken under advisement (whether violating contractual terms of service can be used to support a 1030 violation).

28 August 2009 - Judge Wu issued an opinion granting Drew's motion for judgment of acquittal.

1 H. Dean Steward SBN 85317  
107 Avenida Miramar, Ste. C  
2 San Clemente, CA 92672  
949-481-4900  
3 Fax: (949) 496-6753  
deansteward@fea.net

4 Attorney for Defendant  
5 Lori Drew

6  
7  
8 UNITED STATES DISTRICT COURT  
9 CENTRAL DISTRICT OF CALIFORNIA

10 UNITED STATES,

11 Plaintiff,

12 vs.

13 LORI DREW,

14 Defendant.

Case No. CR-08-582-GW

NOTICE OF MOTION; MOTION TO  
DISMISS INDICTMENT-  
UNCONSTITUTIONAL DELEGATION OF  
PROSECUTORIAL POWER; POINTS AND  
AUTHORITIES

Date: Sept. 4, 2008  
Time: 8:30 AM

16  
17 TO: UNITED STATES ATTORNEY THOMAS O'BRIEN AND ASST. U.S  
18 ATTORNEY MARK KRAUSE, please take notice that on September 4, 2008  
19 at 8:30 AM, defendant, through counsel, will bring the attached  
20 motion to dismiss the indictment in the courtroom of the Honorable  
21 George Wu, United States District Judge, 312 N. Spring St.,  
22 Courtroom 10, Los Angeles, California.

23 Dated: July 23, 2008

s./ H. Dean Steward

24 H. Dean Steward  
25 Counsel for Defendant  
26 Lori Drew  
27  
28

1 MOTION

2 COMES NOW defendant Lori Drew, together with counsel, and  
3 moves this honorable court for an order dismissing the instant  
4 indictment pursuant to Federal Rules of Procedure 12(b). As set  
5 forth below, the indictment violates constitutional due process by  
6 delegating prosecutorial powers, and it must be dismissed.  
7

8 Dated: July 23, 2008

9 San Clemente, California s./ H. Dean Steward  
10 H. Dean Steward  
11 Counsel for Defendant  
12 Lori Drew  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 POINTS AND AUTHORITIES

2  
3 I. BACKGROUND

4 The defense here challenges the government's delegation to the  
5 power to set guidelines and terms of what will be a criminal law  
6 violation to individuals and entities. The public in general, (and  
7 defendant Drew in particular), are denied due process under the  
8 Constitution when private parties, not the government, are given  
9 these rights and powers.

10 II. FACTS

11 According to the indictment, defendant Lori Drew and others  
12 set about creating a MySpace social network on line personal  
13 profile in the Fall of 2006. The profile was of a teenage boy. The  
14 indictment further alleges that Ms. Drew and others set up the  
15 profile to gain information from one M.T.M., a teenager. In setting  
16 up the profile, the government alleges that Ms. Drew and others  
17 violated the terms of service [hereinafter TOS] that MySpace  
18 maintains as a feature of their website. The government theory is  
19 that a violation of any TOS renders any accessing of a website by  
20 the violator to be "unauthorized", and therefore potentially a  
21 violation of 18 USC §1030(a)(2)(C) and (c)(2)(B)(ii) [hereinafter  
22 §1030],

23 The profile was open for 29 days, during which M.T.M. sent  
24 messages back and forth to the fictional person allegedly named  
25 "Josh Evans"<sup>1</sup>. On the last of those 29 days, the messages from

26  
27 <sup>1</sup> The defense believes that at least two other persons and perhaps  
28 as many as four had the "Josh Evans" password and communicated to  
M.T.M. as "Josh Evans".

1 several people to M.T.M., and her responses, became heated, and  
2 M.T.M. soon thereafter took her own life.

3 The facts in this matter are deeply in dispute. For the  
4 purposes of a dismissal motion only, the court is limited to the  
5 four corners of the indictment. U.S. v. Edmonds 103 F.3d 822 (9<sup>th</sup>  
6 Cir. 1996).

### 7 III. DISCUSSION

8 Under §1030, virtually anyone, (be it giant MySpace, the  
9 social network, or an individual computer owner), can determine  
10 whether access to a server or site is authorized, and they can  
11 determine under what circumstances. A computer owner can set the  
12 scope of authorization by contractual language, by a TOS. This can  
13 lead to criminal violations for those who run afoul of the  
14 TOS/contract.

15 Turning to this matter, MySpace dictated, through its TOS,  
16 what acts supposedly constituted a crime. What the government in  
17 its view of §1030 has done is to delegate the responsibility of  
18 deciding what conduct will be criminal to private parties like  
19 MySpace.

20 In *Cybercrime's Scope: Interpreting "Access" and*  
21 *"Authorization" in Computer Use Statutes*, Kerr, 78 N.Y.U.L.Rev.  
22 1596 (2003) Professor Orin Kerr points up the chilling effect of  
23 allowing an entity such as MySpace to anchor and, in truth, dictate  
24 §1030 charges:

25  
26 "Imagine that a Website owner announces [and puts in his  
27 TOS] that only right handed people can view  
28

1 his Website, or perhaps only friendly people.  
2 Under the contract-based approach, a visit to the site  
3 by a left-handed or surly person is an unauthorized  
4 access that may trigger state and federal criminal laws. A  
5 computer owner could set up a public web page, announce that  
6 'no one is allowed to visit my web page', and then refer for  
7 prosecution anyone who clicks on the site out of curiosity. By  
8 granting the computer owner essentially unlimited authority to  
9 define authorization, the contract standard delegates the  
10 scope of criminality to every computer owner."

11  
12 Id. at p. 1650,51  
13  
14

15       Allowing computer owners to set terms that can cause law  
16 violations is similar to the vintage cases in the Supreme Court  
17 where governmental powers were unconstitutionally delegated between  
18 governmental agencies. The Supreme Court invalidated the delegation  
19 of these powers in the 1930's in a series of cases. See Carter v.  
20 Carter Coal Co. 298 U.S. 238 (1936); A.L.A. Schechter Poultry Corp.  
21 v. U.S. 295 U.S. 495 (1935) and Panama Refining Co. v. Ryan 293  
22 U.S. 388 (1935).  
23

24       For example, at issue in Panama Refining was a delegation to  
25 the President of authority to prohibit interstate transportation of  
26 what was known as "hot oil" - oil produced in excess of quotas set  
27 by state law. The problem was that the Act provided no guidance to  
28 the President in determining whether or when to exercise this



1 authority, and required no finding by the President as a condition  
2 of exercise of the authority. Congress "declared no policy, . . .  
3 established no standard, [and] laid down no rule," but rather "left  
4 the matter to the President without standard or rule, to be dealt  
5 with as he pleased." Id. at 293 U.S. at 430.

6 At issue in Schechter was a delegation to the President of  
7 authority to promulgate codes of fair competition that could be  
8 drawn up by industry groups or prescribed by the President on his  
9 own initiative. The codes were required to implement the policies  
10 of the Act, but those policies were so general as to be nothing  
11 more than an endorsement of whatever might be thought to promote  
12 the recovery and expansion of the particular trade or industry. The  
13 President's authority to approve, condition, or adopt codes on his  
14 own initiative was similarly devoid of meaningful standards, and  
15 virtually unfettered. The Act supplied "no standards" for any trade  
16 or industry group, and, unlike other broad delegations that had  
17 been upheld, did not set policies that could be implemented by an  
18 administrative agency required to follow "appropriate  
19 administrative procedure." "Instead of prescribing rules of  
20 conduct, [the Act] authorize[d] the making of codes to prescribe  
21 them." Id. 295 U.S. at 541.

22 Here, §1030 has delegated power, not between branches of  
23 government, but to every day citizens and entities. But like the  
24 older cases above, there are no standards for computer owners when  
25 setting up TOS's. At the same time, however, these owners now have  
26 the power to set guidelines, rules and terms that can, if violated,  
27 cause criminal liability. Such power, by the government's

28

1 interpretation of §1030, is now in the hands of Internet behemoths  
2 like MySpace, or anyone or any entity that can get on the Internet  
3 and set up a rudimentary Website. The enormous danger in this  
4 interpretation is well set out in Professor Kerr's examples, above.

5 In testimony before Congress in 1992, the Vice President and  
6 General Counsel of the Computer and Communications Industry  
7 Association warned, "You do not want to be accidentally taking a  
8 large percentage of the American people, either small businesses or  
9 citizens, into the gray area of criminal law." U.S. v. LaMacchia  
10 871 F. Supp. 535, 544 (D. Mass. 1994), n. 18. The indictment here  
11 does just that, with no due process protections at all. Almost any  
12 computer owner can set up whatever arbitrary and unique rules they  
13 want, and a violation of those rules can lead to a §1030  
14 prosecution.

15 IV. CONCLUSION

16 Simply put, access that merely breaches a contract  
17 conditioning access should not suffice to trigger criminal  
18 liability. If violating user agreements is a crime, millions of  
19 Americans are probably committing crimes on a daily basis and don't  
20 know it.

21 Basing a federal prosecution on TOS violations, on a contract  
22 theory, denies due process, in that "it allows a computer owner to  
23 harness the criminal law at his or her discretion, using his or her  
24 unilateral power to control authorization by contract as a tool to  
25 criminalize any viewpoint of status the owner wishes to target."  
26 *Cybercrime's Scope: Interpreting "Access" and "Authorization" in*

1 Computer Use Statutes supra at p. 1658. Such a delegation is  
2 constitutionally infirm, and the indictment must be dismissed.

3 Dated: July 23, 2008

4 San Clemente, California

s./ H. Dean Steward

H. Dean Steward

Counsel for Defendant

Lori Drew

1 **CERTIFICATE OF SERVICE**

2  
3  
4 IT IS HEREBY CERTIFIED THAT:

5 I, H. Dean Steward, am a citizen of the United States, and am at  
6 least 18 years of age. My business address is 107 Avenida Miramar,  
7 Ste. C, San Clemente, CA 92672.

8 I am not a party to the above entitled action. I have caused,  
9 on July 23, 2008, service of the defendant's:

10 **NOTICE OF MOTION; MOTION TO DISMISS; POINTS AND AUTHORITIES**

11 On the following parties electronically by filing the foregoing  
12 with the Clerk of the District Court using its ECF system, which  
13 electronically notifies counsel for that party.  
14

15 **AUSA Mark Krause**

16  
17 I declare under penalty of perjury that the foregoing is true and  
18 correct.

19 Executed on July 23, 2008

20  
21 H. Dean Steward

22 H. Dean Steward  
23  
24  
25  
26  
27  
28

1 H. Dean Steward SBN 85317  
2 107 Avenida Miramar, Ste. C  
3 San Clemente, CA 92672  
4 949-481-4900  
5 Fax: (949) 496-6753  
6 deansteward@fea.net

7  
8 Attorney for Defendant  
9 Lori Drew

10 UNITED STATES DISTRICT COURT  
11 CENTRAL DISTRICT OF CALIFORNIA

12 UNITED STATES,

13 Plaintiff,

14 vs.

15 LORI DREW

Defendant.

Case No. CR-08-0582-GW

CONSOLIDATED REPLY TO  
GOVERNMENT'S OPPOSITION TO MOTIONS  
TO DISMISS FOR FAILURE TO STATE  
AND OFFENSE; FOR VAGUENESS; FOR  
IMPROPER DELEGATION OF AUTHORITY

16 Comes now defendant, together with counsel, and files this  
17 consolidated reply to the government's oppositions to three motions  
18 on file. Between the defense, Amicus and prosecution, the court now  
19 has 130+ pages of briefing. The defense presents here only a few  
20 key points as to each motion that the defense asks the court to  
21 keep in mind.

22 In addition, the defense joins and adopts the brief filed By  
23 the Amicus.

24 August 18, 2008  
25 San Clemente, California

s./ H. Dean Steward  
H. Dean Steward  
Counsel for Defendant Drew

1 **I. FAILURE TO STATE AN OFFENSE**

2 1. THE FACTS THE GOVERNMENT MAY OR MAY NOT BE ABLE TO PROVE AT  
3 TRIAL ARE NOT RELEVANT FOR THESE MOTIONS

4 In their opposition to all three defense motions, the  
5 government spends 3-4 pages on "facts" they claim they can prove at  
6 trial. The defense submits that many of the "facts" are not true,  
7 and in any event, none of them are relevant for this Court's review  
8 of these motions. U.S. V. Edmonds 103 F.3d 822 (9<sup>th</sup> Cir. 1996).

9 2. THE INDICTMENT FAILS TO ALLEGE *ELEMENTS* OF 1030

10 The point of this motion is that the indictment fails to  
11 allege elements of \$1030. Specifically, the indictment does not  
12 allege, other than a tracking of the statutory language, that  
13 defendant intentionally accessed a computer, or did so without  
14 authorization. On this point alone, the indictment must be  
15 dismissed.

16 3. DEFENDANT DID NOT "KNOW HER CONDUCT VIOLATED THE RULES" OF  
17 MYSPACE AND THE GOVERNMENT HAS UNSUCCESSFULLY PLED KNOWLEDGE

18 Without re-hashing the defense motion already on file, the  
19 point is that the required knowledge on defendant's behalf has not  
20 been pled, other than in the generic language of the statute. The  
21 government tries to cover this glaring hole at page 13, line 23-27,  
22 note 6:

23 "The indictment also describes some of the facts that  
24 show defendant knew her conduct violated the rules  
25 established by MySpace and intended to break those rules. For  
26 example, the indictment alleges how defendant and her co-  
27 conspirators sought to cover up the scheme."

28 Govt. Opposition- Vagueness- p. 13

1 This position makes no sense. Even if true, later efforts to  
2 hide e-mail in no way indicate that defendant or the unindicted  
3 persons knew or were aware of the MySpace TOS. The elements of the  
4 offense must be plainly and concisely pled, not squeezed from an  
5 inference. Federal Rules of Criminal Procedure 7(c)(1).

6 4. THE LaMACCIA CASE IS INSTRUCTIVE AND APPLICABLE HERE

7 Perhaps the biggest failing of the government in this  
8 indictment is the effort to bend a statute (§1030) to fit conduct  
9 that these prosecutors would like to criminalize. This is precisely  
10 what happened in U.S. v. LaMacchia 871 F.Supp 535 (D. Mass. 1994).  
11 The U.S. Attorney's Office in Boston tried to bend the wire fraud  
12 statute to fit facts that just did not violate that statute. The  
13 district court rejected that effort, dismissed the case,<sup>1</sup> and the  
14 Court here should as well.

15 The district court in LaMacchia recognized that copyright law,  
16 at that time, did not contain criminal provisions against non-  
17 commercial infringement. The government here tries to down play  
18 LaMacchia because it was a wire fraud indictment in a copyright

19 /  
20 /  
21 /  
22 /  
23 /

---

24  
25  
26 <sup>1</sup> At various places the government questions the ability of the  
27 motions filed here to give the power to the court to dismiss the  
28 indictment. One need look no further than the LaMacchia case for a  
concrete example for the district court dismissing an indictment  
upon proper showing.

1 case. The government misses the point: prosecutors cannot bend  
2 criminal statutes like §1030 to charge conduct not covered by that  
3 statute.<sup>2</sup>

4 As the Amicus notes:

5 "If Congress wanted to criminalize the conduct at issue  
6 here, it could have. If Congress wanted to give the force of  
7 law to terms of service agreements, it can. But it did not..."  
8 Brief, at p. 21.

## 9 **II. CHARGES ARE VAGUE**

10 1. CASES CITED BY THE GOVERNMENT ON "ACCESS" MISS THE MARK

11 The government must concede that no published opinions in  
12 criminal prosecutions back their view of the definition of access.  
13 The cases the government cited do not support their position:

- 14 • U.S. v. Phillips- no holding on access at all, merely cites  
15 Kansas and Washington state opinions in a footnote
- 16 • Southwest Airlines- not a criminal case; memo order only;  
17 cites dictionary definition
- 18 • Role Models America- civil case; held defendant *did not*  
19 access, under a dictionary definition
- 20 • Am Online, Inc.- civil case; dictionary definition

21 With no case law support, either the government is blazing new  
22 trails, or they have gone too far in their view of "access". The  
23 defense suggests its both.

---

24  
25  
26 <sup>2</sup> The Amicus also points to U.S. v. McDaniel CR-01-638-LGB as  
27 another example of the government (there unsuccessfully) trying to  
28 bend a statute to fit the facts. In LaMacchia, McDaniel and Drew, it  
is clear that statutes have not kept up with technology. The  
solution is not bending the current laws, but rather crafting new,  
appropriate legislation.



1           2. THE DEFENSE DOES DISPUTE THE MEANING OF THE WORDS IN THE  
2 STATUTE

3           The government curiously states in their opposition that,  
4 "Defendant does not seem to dispute the plain meaning of the  
5 statute." Opposition at page 16, line 7-8. The meaning of the words  
6 in the statute (intentionally, access, unauthorized) are very much  
7 in dispute.

8           3. CYBERBULLYING IS NOT A §1030 VIOLATION

9           The Amicus brief explores the legislative history of §1030.  
10 Brief, p. 8-10. The Amicus argues persuasively that the intent of  
11 Congress in enacting §1030 was to prohibit "high tech crimes". The  
12 Amicus highlights the Congressional committee report that  
13 emphasizes concerns about "hackers" who "trespass into" computers  
14 and the inability of "password codes" to protect against this  
15 threat. Brief at p. 8. This legislative history demonstrates the  
16 Congressional intent to prohibit trespass and theft under §1030,  
17 not improper motive or use. Cyberbullying is not, under any  
18 definition, trespass or theft.

19           The government has cited no legislative history to support  
20 their §1030 cyberbullying theories, the heart of this prosecution.  
21 And indeed they cannot. This statute was simply not intended to  
22 prohibit the conduct they seek to criminalize. It was intended as a  
23 straightforward prohibition against computer trespass and theft.

### 24 **III. IMPROPER DELEGATION OF AUTHORITY**

25           1. THE GOVERNMENT HERE DELEGATES PROSECUTORIAL POWER, NOT  
26 LEGISLATIVE

27           As the original defense motion makes clear, the problem is not  
28 a delegation of legislative power, but rather prosecutorial power.

1 Any website owner can, under the government's view in this case,  
2 set terms that can cause a violation of federal laws.

3 2. THE HEART OF ANY §1030 PROSECUTION, UNDER THE GOVERNMENT'S  
4 THEORY, IS THE WEBSITE OWNER

5 In their opposition, the government suggests that a website  
6 owner/creator is peripheral to any §1030 prosecution, and therefore  
7 nothing has been delegated. The flaw in this position is that it is  
8 the website owner himself or herself who *selects and sets* the  
9 critical contractual terms- terms that are then potentially  
10 violated, causing a federal criminal law violation. Website owners  
11 are central to any alleged violation, under the government's theory  
12 in this case. And that is the precise problem: basing criminal  
13 liability on private contract terms [terms of service] invites a  
14 host of difficult, thorny problems and unwanted results. See Amicus  
15 brief, p. 26-36.

16 IV. CONCLUSION

17 For the reasons set out above, in the original motions and in  
18 the Amicus brief, this indictment must be dismissed.

19  
20 August 18, 2008

21 San Clemente, California s./ H. Dean Steward

22 H. Dean Steward  
23 Counsel for Defendant  
24 Lori Drew  
25  
26  
27  
28

1 CERTIFICATE OF SERVICE

2  
3  
4 IT IS HEREBY CERTIFIED THAT:

5 I, H. Dean Steward, am a citizen of the United States, and am at  
6 least 18 years of age. My business address is 107 Avenida Miramar,  
7 Ste. C, San Clemente, CA 92672.

8 I am not a party to the above entitled action. I have caused,  
9  
10 on Aug. 18, 2008, service of the defendant's:

11 **REPLIES TO GOVERNMENT MOTION OPPOSITIONS**

12 On the following parties electronically by filing the foregoing  
13 with the Clerk of the District Court using its ECF system, which  
14 electronically notifies counsel for that party.

15 **AUSA Mark Krause**

16  
17  
18 I declare under penalty of perjury that the foregoing is true and  
19 correct.

20 Executed on Aug. 18, 2008

21 H. Dean Steward

22 H. Dean Steward  
23  
24  
25  
26  
27  
28

1 H. Dean Steward SBN 85317  
2 107 Avenida Miramar, Ste. C  
3 San Clemente, CA 92672  
4 949-481-4900  
5 Fax: (949) 496-6753  
6 deansteward@fea.net

7 Orin S. Kerr  
8 Dist. of Columbia BN 980287  
9 2000 H. Street NW  
10 Washington, DC 20052  
11 202-994-4775  
12 Fax 202-994-5654  
13 okerr@gwu.edu

14 Attorneys for Defendant  
15 Lori Drew

11 UNITED STATES DISTRICT COURT  
12 CENTRAL DISTRICT OF CALIFORNIA

14 UNITED STATES,

15 Plaintiff,

16 vs.

17 LORI DREW,

18 Defendant.

Case No. CR-08-582-GW

RULE 29 MOTION FOR JUDGEMENT OF  
ACQUITTAL

20 Comes now defendant, together with counsel, and moves this Court  
21 under Rule 29 of the federal Rules of Criminal Procedure, for a  
22 judgment of acquittal on all counts. The following material  
23 supplements this motion, also made orally in open court.

24 Dated: Nov. 23, 2008

s./ H. Dean Steward

H. Dean Steward

Orin Kerr

Counsel for Defendant Drew

1 I. STANDARD OF REVIEW

2 The standard of review for a Rule 29 motion is to view the  
3 evidence presented against the defendant "in the light most  
4 favorable to the government to determine whether ' any rational  
5 trier of fact could have found the essential elements of the crime  
6 beyond a reasonable doubt.' " U.S. v. Fretter 31 F.3d 783 (9<sup>th</sup> Cir.  
7 1994), quoting Jackson v. Virginia, 443 U.S. 307, 319 (1979).

8 II. INTENT

9 It is essential to remember the government's theory of the  
10 case. The defendant is on trial for intentionally violating  
11 MySpace's Terms of Service. The government's theory of the case is  
12 that intentionally violating a website Terms of Service is a  
13 federal misdemeanor violation of 18 U.S.C. 1030(a)(2)(C), and that  
14 this misdemeanor becomes a felony when it is undertaken in  
15 furtherance of the tort of intentional infliction of emotional  
16 distress.

17 Incredibly, however, the government has offered no evidence  
18 whatsoever that the defendant or any of the alleged co-  
19 conspirators intentionally violated MySpace's Terms of Service.  
20 Neither the defendant nor any co-conspirator ever read or discussed  
21 MySpace's Terms of Service [partial RT Grills testimony, 32-33].  
22 And without having read MySpace's Terms of Service, it was  
23 impossible for the defendant to know of the exact Terms of Service  
24 that the defendant might have "intentionally" violated. Here, it  
25 is essential to realize that in order to violate a Terms of Service  
26 intentionally, a person must have actual knowledge of the exact  
27 term and then make it her conscious object to violate it. A guess  
28

1 that conduct *might* violate a Term of Service is insufficient.  
2 Further, even knowledge that conduct violates a Term of Service is  
3 insufficient. To violate the Terms of Service intentionally, it  
4 must be the conscious object -- the actual goal of the conduct  
5 -- to violate them. See Model Penal Code §2.02 (distinguishing  
6 intentional conduct from mere knowing conduct). And it is simple  
7 logic that you cannot have a conscious object to violate Terms that  
8 you do not even know with certainty exist.

9 This is equally true under the conspiracy count. For the  
10 defendant to be guilty of engaging in a conspiracy to intentionally  
11 violate Terms of Service, it must be the object of  
12 the conspiracy to violate the Terms of Service. But the  
13 government doesn't even claim that the purpose of the conspiracy  
14 was to violate MySpace's Terms of Service. The government's theory  
15 is that the goal of the conspiracy was to inflict emotional  
16 distress on MTM, but that is facially insufficient:  
17 To support a conspiracy charge, the goal of the conspiracy -- the  
18 aim that the co-conspirators attempted to achieve -- must be to  
19 violate a specific MySpace Term of Service.

20 Evidence that the defendant urged the deletion of the MySpace  
21 account is completely irrelevant to the question before the Court.  
22 The government argues that Drew urged the deletion of the MySpace  
23 account because she realized that she had done something wrong by  
24 violating the Terms of Service. But this is simply bizarre.  
25 M.T.M. had committed suicide, and Drew logically feared that the  
26 account could connect Grills and her to the suicide. As Drew  
27 learned, the connection to the suicide would trigger extraordinary  
28

1 public approbation. The public outcry and attention to this case  
2 has nothing to do with the outcry over the Terms of Service: Drew  
3 has not received hate mail and threats by people furious that she  
4 violated MySpace's Terms of Service. To put it simply, it is  
5 completely absurd to think that Drew acted as she did because she  
6 feared that it might be revealed that she violated the Terms of  
7 Service of a website.

8 III. CONCLUSION

9 For the reasons above and the argument made in open court, the  
10 defense asks this Court to dismiss all four counts under Rule 29,  
11 F.R.C.P.

12 Dated: Nov. 23, 2008

s./ H. Dean Steward

H. Dean Steward

Orin Kerr

Counsel for Defendant Drew

1 **CERTIFICATE OF SERVICE**

2  
3  
4 IT IS HEREBY CERTIFIED THAT:

5 I, H. Dean Steward, am a citizen of the United States, and am at  
6 least 18 years of age. My business address is 107 Avenida Miramar,  
7 Ste. C, San Clemente, CA 92672.

8 I am not a party to the above entitled action. I have caused,  
9 on Nov. 23, 2008, service of the defendant's:

10 **RULE 29 MOTION**

11  
12 On the following parties electronically by filing the foregoing  
13 with the Clerk of the District Court using its ECF system, which  
14 electronically notifies counsel for that party.

15 **AUSA MARK KRAUSE- LA**

16  
17 I declare under penalty of perjury that the foregoing is true and  
18 correct.

19 Executed on NOV. 23, 2008

20  
21 H. Dean Steward

22 H. Dean Steward  
23  
24  
25  
26  
27  
28



1 THOMAS P. O'BRIEN  
United States Attorney  
2 CHRISTINE C. EWELL  
Assistant United States Attorney  
3 Chief, Criminal Division  
MARK C. KRAUSE (Cal. State Bar No. 198142)  
4 Assistant United States Attorney  
Deputy Chief, Cyber and Intellectual  
5 Property Crimes Section  
YVONNE L. GARCIA (Cal. State Bar No. 248285)  
6 General Crimes Section  
1200 United States Courthouse  
7 312 North Spring Street  
Los Angeles, California 90012  
8 Telephone: (213) 894-3493/0719  
Facsimile: (213) 894-8601/0141  
9 E-mail: mark.krause@usdoj.gov  
yvonne.garcia@usdoj.gov

10 Attorneys for Plaintiff  
11 United States of America

12 UNITED STATES DISTRICT COURT  
13 FOR THE CENTRAL DISTRICT OF CALIFORNIA  
14

15 UNITED STATES OF AMERICA,	)	CR No. 08-582-GW
	)	
16 Plaintiff,	)	
	)	<u>GOVERNMENT'S OPPOSITION TO</u>
17 v.	)	<u>DEFENDANT'S MOTION FOR JUDGMENT</u>
	)	<u>OF ACQUITTAL</u>
18 LORI DREW,	)	
	)	
19 Defendant.	)	
	)	
20	)	

21  
22 Plaintiff United States of America, by and through its  
23 counsel of record, United States Attorney Thomas P. O'Brien and  
24 Assistant United States Attorneys Mark C. Krause and Yvonne L.  
25 Garcia, respectfully files its opposition to defendant's motion  
26 for judgment of acquittal pursuant to Federal Rule of Criminal  
27 Procedure 29(a).

28 //

1 This opposition is based on the attached memorandum of  
2 points and authorities, the files and records of this case,  
3 including the testimony and exhibits introduced at trial in this  
4 matter, and any additional evidence or oral argument the Court  
5 may wish to consider.

6 Dated: November 23, 2008

7 Respectfully submitted,

8 THOMAS P. O'BRIEN  
9 United States Attorney

10 CHRISTINE C. EWELL  
11 Assistant United States Attorney  
Chief, Criminal Division

12 /s/  
13 MARK C. KRAUSE  
Assistant United States Attorney

14 YVONNE L. GARCIA  
15 Assistant United States Attorney

16 Attorneys for Plaintiff  
17 United States of America  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1                    MEMORANDUM OF POINTS AND AUTHORITIES

2                    I.

3                    INTRODUCTION

4                    On November 21, 2008, the government completed its case-in-  
5 chief against defendant Lori Drew ("defendant"). Drew is charged  
6 with (1) conspiracy to access protected computers without  
7 authorization or in excess of authorized access to obtain  
8 information, in violation of 18 U.S.C. § 371 (count one); and  
9 (2) intentionally accessing protected computers without  
10 authorization or in excess of authorized access to obtain  
11 information, and doing so in furtherance of a tortious act,  
12 namely, intentional infliction of emotional distress, in  
13 violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(ii) (counts  
14 two through four).

15                    At the close of the government's case, defendant moved for a  
16 judgment of acquittal pursuant to Federal Rule of Criminal  
17 Procedure 29(a) ("Rule 29(a)"). Defendant claims that the  
18 government did not present sufficient evidence that defendant  
19 knew that her accessing of the MySpace servers in Los Angeles,  
20 California, was without authorization or in excess of  
21 authorization because the government has not shown that defendant  
22 read the MySpace Terms of Service ("TOS").<sup>1</sup> The Court reserved  
23 judgment and took the motion under submission in order to review  
24 transcripts of pertinent government witness testimony. The Court

25 \_\_\_\_\_  
26                    <sup>1</sup> The government concedes that it cannot prove that  
27 defendant read the MySpace TOS. As discussed below, however, the  
28 crimes charged do not require proof that defendant read the  
MySpace TOS. The government may, as it has, show that defendant  
knew her access to be unauthorized or in excess of authorized  
access, by way of other evidence.

1 also requested briefing from the parties regarding the standard  
2 it should apply in considering defendant's Rule 29(a) motion.

3 For the reasons described in detail below, defendant's  
4 motion should be denied. First, the government is not required  
5 to prove that defendant read the MySpace TOS in order prove that  
6 she knew her accessing of the MySpace servers was unauthorized or  
7 in excess of authorized access. Second, the government has  
8 presented substantial direct and circumstantial evidence from  
9 which a reasonable juror could infer that defendant knew that she  
10 was accessing the MySpace computers without authorization or in  
11 excess of authorization because knew her conduct in helping to  
12 create a fictitious juvenile account and then use this account to  
13 torment another juvenile, M.T.M., was "illegal," wrong, and in  
14 violation of MySpace's rules, yet continued using the MySpace  
15 account to further this conduct. Because a rational trier of  
16 fact reviewing this evidence and drawing all inferences in favor  
17 of the government could find that the essential elements of the  
18 crimes charged have all been proven beyond a reasonable doubt,  
19 the Court must deny defendant's motion.

20 II.

21 ARGUMENT

22 A. IN RULING ON A MOTION FOR JUDGMENT OF ACQUITTAL, THE COURT  
23 MUST DRAW ALL REASONABLE INFERENCES IN FAVOR OF THE  
GOVERNMENT

24 Rule 29(a) permits a trial court to "enter a judgment of  
25 acquittal on any offense for which the evidence is insufficient  
26 to sustain a conviction." In ruling on a motion for judgment of  
27 acquittal, the court must review the evidence "in the light most  
28 favorable to the government to determine whether 'any rational

1 trier of fact could have found the essential elements of the  
2 crime beyond a reasonable doubt.'" United States v. Freter, 31  
3 F.3d 783, 785 (9th Cir. 1994) (quoting Jackson v. Virginia, 443  
4 U.S. 307, 319 (1979)) (emphasis added); see also United States v.  
5 Iriarte-Ortega, 113 F.3d 1022, 1024 n.2 (9th Cir. 1997); United  
6 States v. Bancalari, 110 F.3d 1425, 1428 (9th Cir. 1997). In its  
7 review of the evidence for this purpose, the court must assume  
8 that the trier of fact could resolve all credibility issues and  
9 any "conflicting inferences" from the evidence in favor of the  
10 government. See United States v. Johnson, 229 F.3d 891, 894 (9th  
11 Cir. 2000).

12 **B. AS A MATTER OF LAW, A DEFENDANT CAN INTENTIONALLY ACCESS A**  
13 **COMPUTER "WITHOUT AUTHORIZATION" OR "EXCEED AUTHORIZED**  
14 **ACCESS" EVEN IF SHE DID NOT READ THE TERMS OF SERVICE THAT**  
15 **DEFINE WHAT CONSTITUTES AUTHORIZED ACCESS**

16 \_\_\_\_\_Section 1030(a)(2)(C) prohibits anyone from intentionally  
17 accessing a computer without authorization or in excess of  
18 authorization, and thereby obtaining information from any  
19 protected computer if the conduct involved an interstate or  
20 foreign communication. 18 U.S.C. § 1030(a)(2)(C). In support of  
21 her Rule 29(a) motion, defendant erroneously argues that the  
22 government presented insufficient evidence at trial to prove that  
23 defendant intentionally accessed the MySpace server without  
24 authorization or in excess of authorization because the  
25 government did not present evidence that defendant read the  
26 MySpace TOS. Proof of that fact is not required, however.

27 The Computer Fraud and Abuse Act ("CFAA") does not  
28

1 explicitly define "without authorization."<sup>2</sup> Courts have  
2 routinely looked to written agreements, including TOS, to  
3 determine whether access of a protected computer is authorized,  
4 unauthorized, or in excess of authorization. In doing so, courts  
5 have suggested that a plain meaning interpretation of "without  
6 authorization" should apply. See, e.g., Calyon v. Mizuho Sec.  
7 USA, Inc., 2007 WL 2618658 (S.D.N.Y. Sept. 5, 2007) ("the plain  
8 language of the statute seems to contemplate that, whatever else,  
9 'without access' and 'exceeds authorized access' would include an  
10 employee who is accessing documents on a computer system which  
11 that employee had to know was in contravention of the wishes and  
12 interests of his employer"); Calence LLC v. Dimension Data  
13 Holdings, 2007 WL 1526349 (W.D. Wash. May 23, 2007) (in case  
14 alleging defendant breached employment and confidentiality  
15 agreements in accessing and disseminating information, holding  
16 "this Court has generally accepted the notion that Congress  
17 intended to encompass actions such as those allegedly taken by  
18 defendant"); Ticketmaster LLC v. RMG Tech., Inc., 507 F.Supp.2d  
19 1096 (C.D. Cal. 2007) (Collins, J.) (violation of terms of  
20 service resulted in "unauthorized access"); Hewlett-Packard Co.  
21 v. Byd:Sign, Inc., No. 05-CV-456, 2007 WL 275476, at \*13 (E.D.  
22 Tex. Jan. 25, 2007) (defendant's conduct violated written  
23 agreements regarding access and were, therefore, unauthorized);  
24 America Online, Inc. v. LCGM, Inc., 46 F. Supp.2d 444, 450-51  
25 (E.D. Va. 1998) (holding that massive email transmissions, or

---

26  
27 <sup>2</sup>Section 1030(e)(6) defines the term "exceeds authorized  
28 access" as "to access a computer with authorization and to use  
such access to obtain or alter information in the computer that  
the accessor is not entitled to so obtain or alter."

1 "spam," sent by customers of the plaintiff were sent without  
2 authorization because the emails violated the terms of service of  
3 plaintiff); Hotmail Corp. v. Van\$ Money Pie, Inc., 1998 WL 388389  
4 (N.D. Cal. Apr. 16, 1998) (misuse of email addresses in violation  
5 of terms of service constituted "unauthorized" access). Put  
6 simply, to access a computer without authorization means "to  
7 access a computer without the approval, permission, or sanction  
8 of the computer's owner." Gov't Proposed Jury Instruction No.  
9 26; see also Webster's New World Dictionary, 3d Collegiate Ed. 92  
10 (1988) (defining "authorization" as "legal power or right,  
11 sanction"); [http://dictionary.reference.com /browse/authorized](http://dictionary.reference.com/browse/authorized)  
12 (defining "authorization" as "permission or power granted by an  
13 authority, sanction"); see also Black's Law Dictionary 1559, 143  
14 8th ed. (defining "unauthorized" as "done without authority" and  
15 "authorize" as "to give legal authority; to empower" and "to  
16 formally approve").

17 TOS, by their very nature, define both authorized and  
18 unauthorized uses of a website. Conduct in accessing a computer  
19 in violation of the terms set forth by the computer's owner is  
20 plainly "without the approval, permission, or sanction" of that  
21 computer owner. MySpace's TOS explicitly prohibit posting the  
22 photograph of a person without that person's consent, harassment,  
23 abusive conduct, encouraging others to harass, and solicitation  
24 of personal information from anyone under the age of 18 - all  
25 activities in which defendant engaged by using the fake MySpace  
26 account. (See Gov't Ex. 3.) As Jae Sung, MySpace's Vice  
27 President of Customer Care, testified, these rules are necessary  
28 to ensure a safe online community. MySpace even has teams of

1 employees dedicated to ensuring that members adhere to the TOS.  
2 Failure to comply results in termination of services and, on  
3 occasion, referral to law enforcement. MySpace's policing of its  
4 website to enforce the TOS makes it clear that access that  
5 involves a violation of the TOS is "without the approval,  
6 permission, or sanction" of MySpace.

7 Although the point at which access becomes "without  
8 authorization" or in excess of authorization is defined by the  
9 MySpace TOS, defendant need not have read the TOS in order for  
10 her conduct to be in violation of the law. As an initial matter,  
11 the statute merely requires that defendant intend to access a  
12 computer without authorization or in excess of authorization --  
13 it does not explicitly mention TOS, nor does it limit in any way  
14 the means by which the intent to engage in unauthorized access  
15 must be established. Nothing in the statute, therefore, can be  
16 read as requiring that a defendant must actually read the TOS  
17 that render her access unauthorized so long as there is  
18 alternative evidence from which a jury can infer this knowledge.

19 Moreover, absent from the statute is any use of the term  
20 Congress has used when it intends to require actual knowledge of  
21 the specific rules that render one's conduct unlawful, namely,  
22 the term "willfulness." A venerable principle of criminal law is  
23 that ignorance of the law is no defense to a criminal charge.  
24 Cheek v. United States, 498 U.S. 192, 199 (1991). This is a  
25 concept that is "deeply rooted in the American legal system."  
26 Id. Where Congress has intended to soften that blow, it has done  
27 so explicitly by ascribing a *mens rea* that requires the  
28 defendant's conduct to be "willful." Id. at 200. The Ninth



1 Circuit has repeatedly held that where a statute does not require  
2 proof of a willful violation, the government is not required to  
3 prove that a defendant has knowledge of the particular law that  
4 has been violated. See, e.g., United States v. Hancock, 231 F.3d  
5 557, 562 (9th Cir. 2002) (affirming district court's refusal to  
6 give instruction that defendant "knew that it was illegal for him  
7 to possess firearms" because prosecution under 18 U.S.C. § 922(g)  
8 does not require proof of willful violation). That section  
9 1030(a)(2)(C) does not contain a willfulness requirement,  
10 therefore, supports the government's position that it is not  
11 required to prove that defendant read the TOS in order for the  
12 jury to find that defendant intentionally accessed the MySpace  
13 server "without authorization" or in excess of authorization, but  
14 may instead prove defendant's knowledge that her access was  
15 unauthorized or in excess of authorization by other means.

16 **C. THE GOVERNMENT HAS PRESENTED SUBSTANTIAL EVIDENCE THAT**  
17 **DEFENDANT KNEW THAT THE CONTINUED USE OF THE MYSPACE ACCOUNT**  
18 **WAS WRONG, IN VIOLATION OF MYSPACE RULES, AND ILLEGAL, YET**  
19 **CONTINUED TO MAINTAIN AND USE IT "WITHOUT AUTHORIZATION" OR**  
20 **IN EXCESS OF AUTHORIZATION**

21 The evidence presented by the government in its case-in-  
22 chief strongly supports the inference that defendant  
23 intentionally accessed the MySpace servers "without  
24 authorization" or in excess of authorization because defendant  
25 was placed on notice that her conduct was wrong, in violation of  
26 the rules of MySpace, and illegal, yet insisted on perpetuating  
27 the scheme using the fake MySpace account. Rational jurors could  
28 find beyond a reasonable doubt, based upon the testimony of  
Ashley Grills, Christina Chu, and Christina Meier that defendant  
intentionally accessed the MySpace servers "without

1 authorization" and in excess of authorization.

2 First, defendant's co-conspirator Ashley Grills twice raised  
3 concerns about the propriety of the "Josh Evans" scheme to  
4 defendant and explained that their conduct was "illegal." Within  
5 days of creating the fake MySpace account, both Ms. Grills and  
6 defendant's own daughter, S.D., told defendant that they were  
7 concerned that they would get in trouble because what they were  
8 doing was "illegal."

9 Q: During the first week after you created the  
10 account did anyone raise any concerns about what  
you were doing?

11 A: Yes.

12 Q: And who was that?

13 A: It was both [S.D.] and I.

14 Q: And who did you raise those concerns with?

15 A: Lori.

16 Q: And what did you tell the defendant?

17 A: That we thought we would get in trouble because  
18 it's illegal to make a fake MySpace.

(Draft Grills Tr. at 14, l. 4-13 (emphasis added).) Defendant,  
19 however, dismissed Ms. Grills' concerns. Defendant told her "it  
20 was fine," and that "people do it all the time." (Id. at 14, l.  
21 16.) (Id. at 15, l. 8-15.) Ms. Grills renewed her objections  
22 later, stating she no longer wanted to be involved. (Id. at 15,  
23 l. 21-22.) Despite this second warning, defendant again assured  
24 Ms. Grills "that it was fine and it didn't matter and [they]  
25 weren't going to get in any trouble." (Id. at 15, l. 24-25.)  
26 Such evidence supports an inference that during the pendency of  
27 the conspiracy, defendant was aware of the rules of MySpace, knew  
28

1 that the scheme was illegal because it violated those rules, but  
2 believed (and so assured Ms. Grills and S.D.) That she need not  
3 worry about the improper conduct because of a perceived lack of  
4 enforcement.

5 Similarly, when defendant visited Michael A's Hair Salon,  
6 she bragged to her hairdresser, Bonnie King, about the fake  
7 MySpace account. According to Dawn Chu's testimony, defendant  
8 explained to Ms. King that she was posing as a boy on MySpace in  
9 order to get back at an unidentified girl. Dawn Chu became upset  
10 and told defendant that her conduct was wrong. Defendant did not  
11 respond and instead continued to use the fake MySpace account. A  
12 rational jury could infer that this represented a third time that  
13 defendant was placed on notice that her conduct in creating adn  
14 using the fake MySpace account was wrong and illegal, and that  
15 defendant's ongoing persistence in using the fake MySpace account  
16 represented intentional access of the MySpace servers "without  
17 authorization" or in excess of authorization.

18 Second, defendant's actions upon learning that M.T.M. had  
19 committed suicide are evidence of consciousness of guilt that  
20 further demonstrate defendant's knowledge that her use of the  
21 MySpace account was unauthorized. After Grills and daughter S.D.  
22 investigated the cause of the ambulances at the Meier home and  
23 told defendant that M.T.M. had committed suicide, defendant "was  
24 kind of quiet for a minute and then her husband started yelling  
25 at [Grills and S.D.] to get rid of the MySpace and then  
26 [defendant] started yelling at [Grills and daughter S.D.] to get  
27 rid of the MySpace." (Draft Grills Tr. at 22, l. 9-11.) The  
28 fact that, immediately after M.T.M.'s death, defendant took steps

1 to evade detection by law enforcement by seeking to destroy  
2 evidence of the fake MySpace account clearly supports an  
3 inference that defendant knew that it was her use of the MySpace  
4 account that rendered her conduct illegal because that use was  
5 unauthorized. Leathers v. United States, 250 F.2d 159, 159, 162  
6 (9th Cir. 1957) (destruction of tax records relevant to  
7 defendant's knowledge of illegal conduct; citing Wigmore on  
8 Evidence); see also United States v. James, 764 F.2d 885, 890  
9 (D.C. Cir. 1985) (destruction of evidence relevant to defendant's  
10 knowledge of illegal conduct related to drug trafficking); United  
11 States v. Robinson, 635 F.2d 981 (2d Cir. 1980) (destruction of  
12 passport relevant to defendant's knowledge of illegal conduct).  
13 Defendant, after all, did not instruct her co-conspirators to  
14 destroy the evidence of other modes of electronic communication  
15 used in communicating with M.T.M., like AOL Instant Messenger,  
16 Xanga, or Yahoo! Messenger, thus demonstrating her knowledge that  
17 the use of the fake MySpace account was materially different and  
18 more culpable, precisely because that use was so patently  
19 unauthorized and wrong. Evidence regarding consciousness of  
20 guilt, combined with the fact that defendant was placed on notice  
21 multiple times that her conduct was wrong, would enable a  
22 rational jury to infer that defendant persisted in using the fake  
23 MySpace account with the required intent of accessing the MySpace  
24 servers "without authorization" and in excess of authorization.

25 Finally, defendant was aware that S.D. had set up her own  
26 fake MySpace account prior to the summer of 2006. Ms. Meier  
27 testified that, prior to creation of the "Josh Evans" MySpace  
28 account, M.T.M. and S.D. created a different MySpace account

1 using the fake name "Kelly." (Draft Meier Tr. at 115, l. 20;  
2 116, l. 8.) The girls portrayed "Kelly" as an 18 year old woman.  
3 The girls established the "Kelly" account so that they could  
4 "talk to boys." (Id. at 116, l. 9.) After learning about the  
5 "Kelly" MySpace account, Ms. Meier contacted defendant "and told  
6 her that Megan was not allowed on the computers at [the Drew]  
7 home." (Id. at 117, l. 10-11.) Soon thereafter, defendant  
8 changed S.D.'s cellphone number because boys from various states  
9 had obtained the number through the "Kelly" MySpace account and  
10 had actually contacted S.D. (Id. at 117, l. 19-24.)

11 Rational jurors could infer that this incident alerted  
12 defendant to the risks posed by the Internet and, specifically,  
13 MySpace. In addition, Ms. Meier called defendant after Ms. Meier  
14 discovered the "Kelly" MySpace account and instructed her not to  
15 allow M.T.M. to use the computers in the Drew home, supporting  
16 the inference that Ms. Meier placed defendant on notice that S.D.  
17 and M.T.M. did something wrong by creating the fake "Kelly"  
18 MySpace account. Despite learning this, defendant nevertheless  
19 created the fake "Josh Evans" MySpace account. A rational jury  
20 viewing this evidence, as well as the fact that defendant was  
21 placed on notice multiple times that her conduct was wrong, and  
22 sought to destroy evidence of the fake "Josh Evans" MySpace  
23 account once she learned of M.T.M.'s suicide, in the light most  
24 favorable to the government, could infer that defendant used the  
25 fake MySpace account with the required intent of accessing the  
26 MySpace servers "without authorization" and in excess of  
27 authorization.

28 //

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

III.

CONCLUSION

For the foregoing reasons, the government respectfully requests that the Court deny defendant's motion for judgment of acquittal pursuant to Rule 29(a).

Dated: November 23, 2008

Respectfully submitted,

THOMAS P. O'BRIEN  
United States Attorney

CHRISTINE C. EWELL  
Assistant United States Attorney  
Chief, Criminal Division

/s/  
\_\_\_\_\_  
MARK C. KRAUSE  
Assistant United States Attorney

YVONNE L. GARCIA  
Assistant United States Attorney

Attorneys for Plaintiff  
United States of America

1 H. Dean Steward SBN 85317  
107 Avenida Miramar, Ste. C  
San Clemente, CA 92672  
949-481-4900  
2 Fax: (949) 496-6753

3 Orin S. Kerr  
Dist. of Columbia BN 980287  
4 2000 H. Street NW  
Washington, DC 20052  
5 202-994-4775  
Fax 202-994-5654  
6 okerr@gwu.edu

7  
8 Attorneys for Defendant  
Lori Drew  
9

10 UNITED STATES DISTRICT COURT  
11 CENTRAL DISTRICT OF CALIFORNIA  
12

13 UNITED STATES,

14 Plaintiff,

15 vs.

16 LORI DREW, Defendant.  
17

Case No. CR-08-582-GW

SUPPLEMENT TO RULE 29 MOTION

18 Comes now defendant, together with counsel, and supplements  
19 her previous Rule 29 motions, made orally at the close of the  
20 government's case, again at the close of the defense case, and  
21 by written motion filed Nov. 23, 2008 [docket entry #96].

22 Dated: Dec. 15, 2008

s./ H. Dean Steward

23 H. Dean Steward  
Orin Kerr  
24 Counsel for Defendant Drew  
25

1  
2  
3 I. INTRODUCTION

4 On Nov. 20, 2008, at the end of the government's case in  
5 chief, counsel moved for dismissal of the charges against the  
6 defendant Lori Drew under Rule 29 of the Federal Rules of  
7 Criminal Procedure. Counsel moved again under Rule 29 at the  
8 close of the defense case, on Nov. 21, 2008. On Nov. 23, 2008,  
9 counsel filed a memorandum providing argument for one of the  
10 bases of the motion, namely the lack of evidence that any  
11 unauthorized access was "intentional." This supplemental  
12 memorandum provides argument for a second basis of the Rule 29  
13 motion: That when the statute is construed properly, there is no  
14 evidence that any access was unauthorized.

15 II. ARGUMENT

16 The prosecution of Lori Drew has been front-page news in  
17 newspapers across the country. It has been a major TV story.  
18 It has been covered extensively on the radio. It has been a  
19 popular topic of heated debate on the Internet. With the trial  
20 now over, and the media hoopla subsided, it is essential to step  
21 back and see what this prosecution is and what it is not.

22 The jury's refusal to convict Lori Drew of any of the  
23 government's felony counts has left the court with only a small  
24 part of the original prosecution. At this stage, emotional



1 distress is no longer part of the case. If this case was ever  
2 about "cyberbullying," the jury's verdict ended that connection:  
3 the government simply failed to meet its burden of proof that  
4 Drew was guilty of any cyberbullying. Instead, the jury's  
5 verdict has left the Court with only one type of behavior that  
6 is allegedly criminal. That conduct is the violation of  
7 MySpace's Terms of Service.

8 In light of the jury's verdict, it is now time for the  
9 court to confront and either approve or reject the government's  
10 novel and breathtakingly broad theory of the Computer Fraud and  
11 Abuse Act. The theory of the prosecution is that breach of a  
12 contractual restriction on the Internet is a federal crime. The  
13 government's view is that breach of a contract to use a computer  
14 makes the computer usage unauthorized: The contract governs  
15 rights to use a computer, so breaching the computer makes  
16 accessing the computer "without right" and therefore a crime.  
17 The question the Court must confront in this motion to dismiss  
18 is whether to endorse or reject the government's novel theory.  
19 *Put simply, the question is this: Is it a federal crime to*  
20 *violate a website Terms of Service?*

21 The correct answer should be a resounding no.

22 A. Violations of Contractual Terms Such as Terms of Service Do  
23 Not Make Access Unauthorized.

1 Breaching a contractual term does not make access  
2 unauthorized because crimes punishing conduct "without  
3 authorization" or "without consent" have a well-established and  
4 specific meaning -- a meaning that the government's broad  
5 theory simply ignores. When Congress or a state legislature  
6 punishes an act when it occurs "without authorization," that act  
7 is prohibited only when the person or business that can grant  
8 authorization has *actually declined or failed to give*  
9 *permission*.

10 If a person or business actually *grants* permission for the  
11 act, conditioned on some understanding that turns out to be  
12 false, then the act is *still authorized* for the purposes of  
13 criminal law. See Rollins M. Perkins & Ronald N. Boyce,  
14 Criminal Law 1075-84 (3d ed 1982); Theofel v. Farey-Jones, 359  
15 F.3d 1066, 1073 (9th Cir. 2004). As one court summarized,  
16 "whenever lack of consent is a necessary element of a crime, the  
17 fact that consent is obtained through misrepresentation will not  
18 supply the essential element of nonconsent." People v. Cook,  
19 228 Cal.App.2d 716, 719 (1964). In this case, MySpace permitted  
20 Ashley Grills to create an account and permitted Grills to  
21 access MySpace. By allowing the account and giving its users  
22 access to MySpace, MySpace affirmatively authorized the access  
23 to its computers. The fact that the account breached a  
24

1 contractual restriction does not transform that authorized  
2 access into an unauthorized access.

3 Because computer crimes are new, the cases that best  
4 illustrate this principle are found in other areas of criminal  
5 law that use the same element of lack of authorization or  
6 consent. Perhaps the most analogous cases involve the crime of  
7 taking a vehicle of another without the owner's consent. See,  
8 e.g., Cal. Vehicle Code § 10851. In particular, consider the  
9 cases in which a person uses fraud, misrepresentation, and  
10 trickery to persuade a car owner into handing over the keys. The  
11 trickster is then charged with taking the automobile of another  
12 without the owner's consent. In these cases, the courts have  
13 held that the trickster is not liable for taking the car  
14 "without consent" as a matter of law. Because the owner handed  
15 over the keys, giving the defendant permission to use the car,  
16 the use of the car was authorized rather than unauthorized for  
17 purposes of criminal law. See, e.g., People v. Cook, 228 Cal  
18 App.2d 716 (1964) (Burke, P.J.) (defendant who purchased car by  
19 misrepresenting his identity not guilty of auto theft, as taking  
20 of car was with consent of seller).

21 People v. Donell, 32 Cal.App.3d 613 (1973), is particularly  
22 relevant to this case. In Donell, the defendant allegedly  
23 rented a Hertz rental car using a stolen ID and a stolen Hertz  
24 credit card. The rental contract required the person renting

1 the car to make only truthful representations. The defendant  
2 rented the car in violation of this contractual term, however:  
3 While his real name was Jon Donell, the defendant pretended that  
4 he was "Ernest Carl Johnson." At trial, the judge instructed  
5 the jury that if the jury believed that the defendant had  
6 obtained the car by fraud, then the contract was violated and  
7 the taking of the car was without consent. The Court of Appeal  
8 reversed, applying the usual rule that "fraudulently induced  
9 consent is consent nonetheless." Id. at 617. Although Donell  
10 had rented the car in violation of the rental contract, the  
11 rental company had in fact consented to him taking the car.  
12 The fact that the consent was obtained by fraud did not make the  
13 taking unauthorized as a matter of law. Id.

14 The same principle applies to the proper interpretation of  
15 statutes prohibiting unauthorized access to a computer, as the  
16 Ninth Circuit recognized in Theofel. Access to a computer is  
17 not unauthorized merely because it violates a contract. To be  
18 sure, such access may fraudulently induce the computer owner to  
19 grant access, which under contract law would generally void the  
20 contract between the computer owner and the computer user. See,  
21 e.g., Extra Equipamentos E Exportacao Ltda. v. Case Corp. 541  
22 F.3d 719, 726 (7th Cir. 2006) (Posner, J.) ("[T]he remedy for  
23 fraud in the inducement is to rescind the contract."). Criminal  
24 law is different, however. In criminal law, fraud in the

1 inducement does not make the access unauthorized. See Rollins  
2 M. Perkins & Ronald N. Boyce, Criminal Law 1075-84 (3d ed 1982).

3 B. The Government Failed to Establish Unauthorized Access in  
4 this Case.

5       Construing the evidence in the government's favor, Lori  
6 Drew and Ashley Grills were at most in the same position as Jon  
7 Donell. Like Donell, they obtained property through  
8 misrepresentation of identity that breached a contract. Just as  
9 with Donell, their conduct was not without the authorization of  
10 the property owner. MySpace gave Grills access just like Hertz  
11 gave Donell access. The fact that it was not really "Josh  
12 Evans" registering the account is no more relevant to  
13 authorization than was the fact that it was not "Ernest Carl  
14 Johnson" who rented the car in Donell. In both cases, the  
15 property owner permitted the defendant to control the property:  
16 The access was authorized even though it violated a contractual  
17 restriction on access.

18       This important legal principle explains why most Internet  
19 users are not criminals for the way they send e-mail and surf  
20 the web. Violating Terms of Service by providing false  
21 information to register an account is extremely common online.  
22 Even the founder of MySpace, Tom Anderson, violated that Term of  
23 Service with his own MySpace profile: Anderson knowingly and  
24

1 intentionally entered in a fake age in his MySpace profile,  
2 perhaps to appear younger to the youthful audience of MySpace  
3 users. Jessica Bennett, *Is Age Just A Number?*, Newsweek,  
4 November 5, 2007, available at <http://www.newsweek.com/id/62330>.  
5 Anderson's conduct was not criminal for the same reason that  
6 Drew's conduct and the similar conduct of millions of Americans  
7 is not criminal: A website Terms of Service can define the  
8 contract between owner and user, but it does not define the  
9 scope of criminal law.

10 The government's case in chief was based on the theory that  
11 Drew committed a crime by violating MySpace's Terms of Service.  
12 This theory must be rejected as a matter of law. When it is  
13 rejected, it becomes clear that the government did not provide  
14 any evidence by which a rational jury could find that Drew  
15 committed an unauthorized access into MySpace's computers.

16 /  
17 /  
18 /  
19 /  
20 /  
21 /  
22 /

1 III. CONCLUSION

2 For these reasons, and for the reasons explained in  
3 counsel's earlier written and oral arguments, the Motion to  
4 Dismiss under Rule 29 should be granted.

5 Dated: Dec. 15, 2008

s./ H. Dean Steward

6 H. Dean Steward  
7 Orin Kerr  
8 Counsel for Defendant  
9 Lori Drew  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 **CERTIFICATE OF SERVICE**

2  
3 IT IS HEREBY CERTIFIED THAT:

4 I, H. Dean Steward, am a citizen of the United States, and am at  
5 least 18 years of age. My business address is 107 Avenida  
6 Miramar, Ste. C, San Clemente, CA 92672.  
7

8 I am not a party to the above entitled action. I have  
9 caused, on Dec. 15, 2008, service of the defendant's:

10 **SUPPLEMENT TO RULE 29**

11 On the following parties electronically by filing the foregoing  
12 with the Clerk of the District Court using its ECF system, which  
13 electronically notifies counsel for that party.  
14

15 **AUSA MARK KRAUSE- LA**

16  
17 I declare under penalty of perjury that the foregoing is true  
18 and correct.

19 Executed on DEC. 15, 2008

20 H. Dean Steward

21 H. Dean Steward  
22  
23  
24  
25  
26  
27  
28



1 H. Dean Steward SBN 85317  
2 107 Avenida Miramar, Ste. C  
3 San Clemente, CA 92672  
4 949-481-4900  
5 Fax: (949) 496-6753

6 Orin S. Kerr  
7 Dist. of Columbia BN 980287  
8 2000 H. Street NW  
9 Washington, DC 20052  
10 202-994-4775  
11 Fax 202-994-5654  
12 okerr@gwu.edu

13 Attorneys for Defendant  
14 Lori Drew

15 UNITED STATES DISTRICT COURT  
16 CENTRAL DISTRICT OF CALIFORNIA

17 UNITED STATES,

18 Plaintiff,

19 vs.

20 LORI DREW

21 Defendant.

Case No. CR-08-0582-GW

SECOND SUPPLEMENT TO RULE 29  
MOTION IN LIGHT OF NEW CASELAW

22 Comes now counsel for defendant Lori Drew, and submits the  
23 following supplemental points and authorities, specifically  
24 outlining new case law on the issue.

25 Dated: Feb. 19

26 s./ H. Dean Steward  
27 H. Dean Steward  
28 Orin Kerr  
Counsel for Defendant  
Lori Drew

1  
2 I. Introduction

3       The Court held oral argument on the Defendant's Motion to  
4 Dismiss on January 8, 2009. Since that date, three new federal  
5 court decisions have been handed down that reject the broad reading  
6 that the United States seeks to impose on the Computer Fraud and  
7 Abuse Act, 18 U.S.C. § 1030.

8  
9 II. Three New Decisions Have Been Handed Down in the Last Month  
10 That Reject the Broad Construction of Unauthorized Access.

11       The three new cases concern the most common fact pattern in  
12 the civil caselaw applying unauthorized access statutes. In these  
13 cases, an employee at one company decides to leave; the employee  
14 then accesses the company's computers in the course of preparing to  
15 leave to join a competitor company; and the employee then uses the  
16 employer's confidential information at the new job. As noted in  
17 the prior briefing on this issue, courts are deeply divided on  
18 whether such facts should lead to civil liability under 18 U.S.C. §  
19 1030. Initially, before 2007, several courts said "yes." Since  
20 2007, however, most courts have said "no."

21       The argument of the United States in this criminal case relies  
22 in significant part on the earlier civil cases saying "yes."  
23 Indeed, in its January 5, 2009 Sur-Reply, the United States tried  
24 to dismiss the many cases saying "no" as if they were outliers.  
25 According to the United States, back on January 5, "that line of  
26 cases, which at best must be considered a minority view, is  
27 contrary to the plain language of the statute, its legislative  
28

1 history, and to cases from this district." Government's Sur-Reply  
2 at 8 n. 4 (emphasis added).

3 In light of the Government's position in its Sur-Reply, the  
4 Court should be aware of the following three new cases, all handed  
5 down just in the last month, further rejecting the broad reading of  
6 18 U.S.C. § 1030.

7  
8 A) U.S. Bioservices Corp. v. Lugo, No. 08-2342-JWL, - F. Supp.2d  
9 - , 2009 WL 151577 (D. Kan. January 21, 2009).

10 In this case, District Judge Lungstrum dismissed in part  
11 Section 1030 claims brought by an employer against a former  
12 employee. In rejecting the broad reading of Section 1030, Judge  
13 Lungstrum wrote:

14  
15 Neither side to the present dispute has acknowledged  
16 this clear split in the caselaw or argued why this court  
17 should favor one line of cases over the other; instead,  
18 each side merely attempts to distinguish factually the  
19 "non-controlling" cases cited by the other. Thus, the  
20 parties have offered little help in resolving this  
21 conflict.

22 After reviewing the cases, this court finds  
23 persuasive the reasoning of the courts in the latter  
24 line of cases [adopting the narrower reading of the  
25 statute]. Accordingly, the court follows their lead in  
26 holding that, under these provisions of the CFAA, access  
27 to a protected computer occurs "without authorization"  
28 only when initial access is not permitted, and a

1 violation for "exceeding authorized access" occurs only  
2 when initial access to the computer is permitted but the  
3 access of certain information is not permitted

4 . . . [T]he legislative history of the statute  
5 supports the court's narrow interpretation. The CFAA was  
6 intended as a criminal statute focused on "hackers" who  
7 trespass into computers, and the statute deals with  
8 unauthorized access in committing computer fraud rather  
9 than the mere use of a computer.

10 . . .

11 As the other courts have noted, this interpretation  
12 "has the added benefit of comporting with the rule of  
13 lenity," which might apply in light of the CFAA's  
14 criminal provisions.

15  
16 Id. at \*3-4, \*4 n.5 (internal citations omitted).

17  
18 B) Lasco Foods, Inc. v. Hall and Shaw Sales, Marketing &  
19 Consulting, LLC, NO. 4:08CV01683 JC, 2009 WL 151687 (E.D.Mo.  
20 January 22, 2009).

21 In this case, District Judge Hamilton granted a motion to  
22 dismiss counts brought under both Section 1030 and the analogous  
23 Section 2701, the unauthorized access statute found in the Stored  
24 Communications Act. Judge Hamilton adopted the narrow  
25 interpretation of unauthorized access statutes found in Sherman &  
26 Co. v. Salton Maxim Housewares, Inc., 94 F.Supp.2d 817 (E.D. Mich.  
27 2000). In Sherman & Co., the court had held that deception alone  
28 was not enough to trigger unauthorized access. To impose liability

1 under unauthorized access statutes, "the offender must have  
2 obtained the access to private files without authorization (e.g.,  
3 using a computer he was not to use, or obtaining and using someone  
4 else's password or code without authorization)." Id. at 821.

5 Judge Hamilton applied that same principle to the employer's  
6 claim that the employee had practiced deception by pretending to  
7 have a business reason to access the employer's files. According  
8 to Judge Hamilton, this was insufficient to constitute unauthorized  
9 access:

10  
11 [T]he thrust of Plaintiff's claim is the generalization that  
12 Defendants obtained information for improper purposes. See,  
13 e.g., Compl., 41 ("while Defendant Hall was still employed by  
14 Lasco, he attempted, through deception, to obtain reports from  
15 one of Lasco's [b]rokers"). This "deception," as pled, however,  
16 is not a [§ 2701] violation. "Where a party consents to  
17 another[']s access to its computer network, it cannot claim  
18 that such access was unauthorized." Sherman & Co., 94 F.Supp.2d  
19 at 821. Lasco afforded Defendants access to its computers,  
20 networks and information, which they utilized throughout their  
21 employment. Plaintiff has not alleged anything to the contrary.

22  
23 Id. at \*3 (dismissing SCA claim). See also id. at \*6 (same result  
24 for CFAA claim).

25  
26  
27 C) Bridal Expo, Inc. v. Van Florestein, NO. CIV.A. 4:08-CV-03777,  
28 2009 WL 255862 (S.D. Tex. February 3, 2009).

1  
2 In this case, Judge Ellison rejected the broad reading of  
3 Section 1030 in the course of denying a preliminary injunction:  
4

5 The Court acknowledges that other circuits have approved  
6 the use of the CFAA to reach employees who have obtained  
7 information in violation of their confidentiality  
8 agreements and have extended this reasoning to breaches  
9 of the duty of loyalty to employers. The Fifth Circuit  
10 has not yet taken a position on the issue, but given the  
11 persuasive arguments in Lockheed [v. L-3 Communications  
12 Corp., 6:05-cv-1480-ORL-31, 2006 WL 2683058 (M.D. Fla.  
13 Aug.1, 2006)], and the rule of lenity, given that the  
14 CFAA is also a criminal statute, the Court declines to  
15 read the CFAA to equate "authorization" with a duty of  
16 loyalty to an employer such that the CFAA is applicable  
17 to this case.  
18

19 Id. at \*10.  
20  
21

22 III. The New Decisions Rejecting the Government's View Reflect the  
23 Now-Dominant Interpretation of 18 U.S.C. § 1030.

24 This criminal prosecution is based entirely on the  
25 Government's attempt to take a set of civil cases adopting a broad  
26 reading of 18 U.S.C. § 1030 and to apply them jot-for-jot in the  
27 context of criminal law. As explained in its briefing, those very  
28 broad civil cases cannot be applied in the criminal setting in

1 light of the three related "fair warning" canons for interpreting  
2 criminal statutes: vagueness, the rule of lenity, and overbreadth.

3 The three cases decided just in the last month showcase the  
4 weakness of the Government's approach even as a matter of civil  
5 law. The clear trend even in the civil cases is to reject the  
6 broad reading of the statute that the Government is urging in this  
7 case.<sup>1</sup> See also Condux Intern., Inc. v. Haugum, 2008 WL 5244818 (D.  
8 Minn., December 15, 2008) (rejecting broad view of 18 U.S.C. §1030  
9 and embracing narrow view in light of lenity concerns that arise in  
10 the interpretation of criminal statutes); Black & Decker, Inc. v.  
11 Smith, 568 F.Supp.2d 929 (W.D. Tenn. 2008) (same); Shamrock Foods  
12 Co. v. Gast, 535 F.Supp.2d 962 (D. Ariz. 2008) (same); American  
13 Family Mut. Ins. Co. v. Rickman, 554 F.Supp.2d 766 (N.D. Ohio 2008)  
14 (same).

15 The reason for the trend is easy to identify. The early civil  
16 cases did not appreciate that the CFAA is a criminal statute, so  
17 courts adopted very broad contractual interpretations of the  
18 statute that created a broad civil cause of action. Eventually,  
19 however, courts began to appreciate that they should be  
20 interpreting the CFAA in a civil setting so as to match how the  
21 statute should be construed in a criminal setting. After courts  
22  
23  
24

---

25 <sup>1</sup> In contrast, counsel has found only one case decided in the  
26 last month adopting the broader view of 18 U.S.C § 1030. See Ervin  
27 & Smith Advertising and Public Relations, Inc. v. Ervin, 2009 WL  
28 249998 (D. Neb. Feb. 3, 2009). However, unlike most of the cases  
on this topic in the last year, that decision does not even  
acknowledge the deep split in the cases. As a result, it does not  
justify its approach or confront the contrary argument. See id. at  
\*8.

1 began to realize this, around 2006,<sup>2</sup> the direction of the caselaw  
2 shifted dramatically: The clear trend has become to reject the  
3 broad view and embrace a narrower construction.

4 The United States may wish that the cases rejecting its view  
5 are outliers, or as the Government put it last month, "at best a  
6 minority view." However, those narrow cases have become the  
7 dominant reading of the statute in district courts across the  
8 country. The three new cases decided in the last month reinforce  
9 the trend. This Court should follow the clearly emerging majority  
10 view that the CFAA should be construed narrowly instead of the  
11 increasingly rejected view that the statute should be construed  
12 broadly.

13  
14 IV. Conclusion

15 For the above reasons, the remaining three misdemeanor counts  
16 must be dismissed pursuant to Fed. R. Crim. Pro. 29.

17  
18 Dated: Feb. 19, 2009

s./ H. Dean Steward

H. Dean Steward  
Orin Kerr  
Counsel for Defendant Drew

27  
28 <sup>2</sup> The turning point appears to have been the careful and  
scholarly opinion of Judge Presnell in Lockheed Martin v. Speed,  
2006 WL 2683058, 81 U.S.P.Q.2d 1669 (M.D. Fla. 2006).



1 **CERTIFICATE OF SERVICE**

2  
3  
4 IT IS HEREBY CERTIFIED THAT:

5 I, H. Dean Steward, am a citizen of the United States, and am at  
6 least 18 years of age. My business address is 107 Avenida Miramar,  
7 Ste. C, San Clemente, CA 92672.

8 I am not a party to the above entitled action. I have caused,  
9  
10 on Feb. 20, 2009, service of the defendant's:

11 **Second Supplement to Rule 29**

12 On the following parties electronically by filing the foregoing  
13 with the Clerk of the District Court using its ECF system, which  
14 electronically notifies counsel for that party.

15 **AUSA Mark Krause- LA**

16  
17 I declare under penalty of perjury that the foregoing is true and  
18 correct.

19  
20 Executed on Feb. 20, 2009

21 H. Dean Steward

22 H. Dean Steward  
23  
24  
25  
26  
27  
28

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**RULING: Prosecution Motion  
To Admit Evidence**

18 July 2012

The Government moves to pre-admit the following evidence enclosed to Appellate Exhibit 160:

1. Enclosure 8: Information Awareness screenshot reflecting the user profile of Bradley Manning and the dates of his information awareness training. The record is authenticated by attestation certificate from Willco Technologies, Inc.
2. Enclosure 9: U.S. Information Assurance Virtual Training screenshot reflecting the user profile of Bradley Manning. The record is authenticated by NACON Consulting.
3. Enclosure 11: Joint Asset Movement Management System (JAMMS) Movement Report by Person – 204 records returned for Bradley Manning. The record is authenticated by U.S. ARCENT GI SAMO Section, Camp Arifjan, Kuwait.
4. Classified enclosures: Army Counterintelligence (ACIC) Access Logs, ACIC Server Logs, Central Intelligence Agency (CIA) WIRE Logs, and Centaur Logs. Each of these logs is authenticated by a records custodian from the relevant agency.

Government proffers that the above evidence is admissible as machine generated data and as properly authenticated business records. Defense objects on the ground that the screenshots are testimonial statements in violation of the confrontation clause and are not business records because the business entity did not maintain the data in a snapshot or log format and the data query by law enforcement for particular information from an existing data base makes that information a testimonial statement.

#### **Findings of Fact:**

1. All of the above records were maintained by the various entities in databases for business purposes. The data was collected prior to or contemporaneous with the dates of the charged offenses and was maintained by the entity for business purposes before the query for information by law enforcement.

APPELLATE EXHIBIT 216  
PAGE REFERENCED: \_\_\_\_\_  
PAGE     OF     PAGES

### **The Law:**

1. The Sixth Amendment precludes testimonial hearsay from coming into evidence against an accused without cross-examination of the declarant unless (1) the declarant is unavailable and (2) the declarant was subject to prior cross examination. *U.S. v. Sweeney*, 70 M.J. 296 (C.A.A.F. 2011).
2. A statement is testimonial if made under circumstances which would lead an objective witness reasonably to believe the statement would be available for use at a later trial. A document created solely for an evidentiary purpose made in aid of a police investigation is testimonial. While formalized certifications of results in lab reports are testimonial, machine generated data and printouts are not statements and, thus, they are not hearsay. *Sweeney*, 70 M.J. at 301; *U.S. v. Foerster*, 65 M.J. 120 (C.A.A.F. 2007) (affidavit filled out by victim of check fraud pursuant to internal bank procedures admissible as non-testimonial business record even if later turned over to law enforcement.).

### **Conclusions of Law:**

1. The fact that information maintained on a business related database is pulled from that database in a snapshot format at the request of a law enforcement query does not transform machine generated data into a testimonial statement. It is the nature of the data at issue not the form of the query, the fields of the query, or who made the query that determines whether the information is machine generated, a statement, or a testimonial statement.
2. Unlike the cover memorandum and results certification that were held to be testimonial statements in *Sweeney*, the machine generated data offered for admission by the Government in this case contains no additional representations or certifications that were not machine generated.
3. The records offered for admission by the Government are machine generated and not statements. They are properly authenticated. If the Government offers evidence to show their relevance, the exhibits are admissible.

So **Ordered** this 18<sup>th</sup> day of July, 2012.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

**von Elten, Alexander S. CPT USA JFHQ-NCRMDW SJA**

---

**From:** Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA  
**Sent:** Tuesday, July 17, 2012 7:19 PM  
**To:** David Coombs; Lind, Denise R COL USARMY (US); Williams, Patricia CIV JFHQ-NCR/MDW SJA; Jefferson, Dashawn MSG USARMY (US)  
**Cc:** Hurley, Thomas F MAJ OSD OMC Defense; 'Tooman, Joshua J CPT USARMY (US)'; Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA  
**Subject:** RE: United States v. Martinelli Question (UNCLASSIFIED)  
**Attachments:** US v. Rauscher.pdf

Classification: UNCLASSIFIED

Caveats: NONE

Ma'am,

Attached is United States v. Rauscher, decided by CAAF on 18 June 2012. The Government believes this case is more directly on point. In this case, the Government failed to plead the terminal element of a 134 offense (Assault with intent to commit murder), but the accused was found guilty of a lesser-included offense (Article 128). CAAF affirmed the conviction because the accused was on notice of the lesser-included offense in the specification.

Respectfully,

CPT Joe Morrow  
Trial Counsel  
U.S. Army Military District of Washington  
Phone: 202-685-1975  
NIPR: jodean.morrow@jfhqncr.northcom.mil  
SIPR: jodean.morrow@jfhqncr.northcom.smil.mil

-----Original Message-----

**From:** David Coombs [mailto:coombs@armycourtmarshialdefense.com]  
**Sent:** Monday, July 16, 2012 7:49 PM  
**To:** Lind, Denise R COL USARMY (US); Williams, Patricia CIV JFHQ-NCR/MDW SJA; Jefferson, Dashawn MSG USARMY (US)  
**Cc:** Hurley, Thomas F MAJ OSD OMC Defense; 'Tooman, Joshua J CPT USARMY (US)'; Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA  
**Subject:** United States v. Martinelli Question

Ma'am,

I've had an opportunity to look at the United States v. Martinelli case that you asked me about today in oral argument, and do not believe that it can be read to support the proposition that the Government is entitled to a lesser-included offense for a fatally defective specification. First, as I indicated in oral argument today, the context in which Martinelli was decided is very different than the context in which the issue presents itself here. In Martinelli, the court was assessing the providence of the accused's guilty plea after a case was decided; it was not assessing whether the government

was entitled to an instruction on a lesser-included offense at the outset of the case where the court has found as a fact that the evidence falls short of establishing a legally cognizable defense.

More importantly, though, the reason why the offense was not cognizable in Martinelli is very different than the reason why it is not cognizable here. This difference means that an instruction on the lesser included offense might have been appropriate in Martinelli, but not in the instant case. In Martinelli, the accused was charged under clause 3 with violating the Child Pornography Prevention Act (CPPA) for certain acts he was alleged to have committed while in Germany. After the accused pled guilty to the specifications, the court determined that the CPPA could not apply extraterritorially to the conduct at issue; hence, the clause 3 offenses were not cognizable. The court upheld clause 1 and 2 offenses as being lesser-included offenses of the clause 3 offense.

However, it is important to look at the specifications in Martinelli to understand why they could survive in that case and why they cannot survive in the instant case. The specifications in Martinelli were as follows:

Specification 1: knowingly mailing, transporting or shipping child pornography in interstate or foreign commerce (by computer) in violation of § 2252A(a)(1) (specifically, sending images over the Internet from the Network Internet Café in Darmstadt, Germany);

Specification 2: knowingly receiving child pornography that has been mailed, shipped or transported in interstate or foreign commerce (by computer) in violation of § 2252A(a)(2)(A) (specifically, downloading images from the Internet in the Network Internet Café in Darmstadt, Germany);

Specification 3: knowingly reproducing child pornography for distribution through the mails, or in interstate or foreign commerce (by computer) in violation of § 2252A(a)(3) (specifically, downloading images from the Internet; copying them to hard drive and transmitting the copied files to approximately twenty individuals over the Internet in the Network Internet Café in Darmstadt, Germany);

Specification 4: knowingly possessing child pornography on land and in a building used by and under the control of the United States Government in violation of § 2252A(a)(5)(A) (specifically, possessing approximately fifty diskettes containing child pornography in buildings at the Cambrai Fritsch Kaserne).

Notably, once the judge removed the reference to "in violation of [the CPPA]," the underlying factual acts could still be proved so as to form the basis for an Article 134 offense. In other words, in Martinelli, it wasn't the Government's underlying theory that was deficient. It was simply that the statute did not extend so as to cover acts outside the continental United States.

Otherwise stated, even though the offenses were not cognizable as crimes under the CPPA, the factual acts underlying the original specifications could still be proven and made the basis for a lesser-included offense under Article 134. For instance, under specification 1, the government was still capable of proving that the accused "knowingly mailing, transporting or shipping child pornography in interstate or foreign commerce (by computer)" and that such conduct was prejudicial to good order and discipline. Removal of the offending statute (the CPPA) from the specification did not change the ability of the government to prove the underlying offense.

In the instant case, the factual acts underlying the original specification cannot be proven because the conduct involves "exceeding authorized access" as defined by section 1030. In other words, the specification cannot be proved simply by removing reference to section 1030 as the court did in

Martinelli and other cases like . . . See United States v. Monette, 2007 WL 6625267, \*1 (Army Ct. Crim. App.) ("Our court modified the findings of guilty to Specifications 8, 9, 11, 12, and 13 of Additional Charge II by deleting all Title 18 nomenclature referring to the CPPA, and, for each affected specification, affirmed a lesser-included simple disorder under Article 134") (emphasis supplied).

For instance, in specification 13 of Charge II, the Government pleads that PFC Manning:

did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, having knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer, and by means of such conduct having obtained . . . more than seventy-five classified United States Department of State cables, willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1).]

If the Court were simply to remove the language "in violation of 18 U.S. Code Section 1030(a)(1)" from the specification as did the court in Martinelli, the Government would still not be able to prove the offense because the offense derives from section 1030 and "exceeds authorized access" is defined by the terms of that statute. Thus, this court cannot simply create a lesser-included offense by deleting the Section 1030 "nomenclature" from the specification as the court did in Martinelli.

In order to state an Article 134 offense based on this conduct, the Government would actually need to change the specification to allege some other conduct not in the specification (e.g. the accused used Wget to obtain the cables). In other words, we would be dealing with an amendment to the specification and not a lesser-included offense. The Defense submits that this would be a major amendment under R.C.M. 603 that cannot be made over the objection of the accused.

To the Defense's knowledge, there is no military case that has permitted the government to proceed with lesser-included offense of a clause 3 offense which is not legally cognizable because the Government does not have the factual evidence to proceed. Specifically, there is no case (Martinelli included) where a court has determined pretrial that the Government doesn't have any evidence for an essential element of an offense and nevertheless has allowed the government to go forward with an uncharged lesser-included offense.

Accordingly, the Defense submits that Martinelli does not permit this Court to find a lesser-included offense where the entire theory underlying the specification is deficient. Any Article 134 offense would require a major amendment to the specification which is not permitted over the objection of the accused.

v/r

David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282

coombs@armycourtartialdefense.com

www.armycourtartialdefense.com <<http://www.armycourtartialdefense.com/>>

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

Classification: UNCLASSIFIED

Caveats: NONE

UNITED STATES, Appellee

v.

Jeremy L. RAUSCHER, Machinist's Mate Second Class  
U.S. Navy, Appellant

No. 12-0172

Crim. App. No. 201100684

United States Court of Appeals for the Armed Forces

Argued May 16, 2012

Decided June 18, 2012

PER CURIAM

Counsel

For Appellant: Captain Michael D. Berry, USMC (argued).

For Appellee: Captain David N. Roberts, USMC (argued); Colonel Kurt J. Brubaker, USMC, Lieutenant Benjamin J. Voce-Gardner, JAGC, USN, and Brian K. Keller, Esq. (on brief).

Military Judge: J. Kirk Waits

THIS OPINION IS SUBJECT TO REVISION BEFORE FINAL PUBLICATION.



PER CURIAM:

Appellant was charged under Article 134, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 934 (2006), with assault with intent to commit murder but convicted, contrary to his pleas, of assault with a deadly weapon or other means or force likely to produce death or grievous bodily harm, under Article 128, UCMJ, 10 U.S.C. § 928 (2006). We granted review to consider whether "aggravated assault is a lesser included offense of an Article 134 specification that fails to allege the terminal element" -- that Appellant's conduct was prejudicial to good order and discipline or was of a nature to bring discredit upon the armed forces. We hold that Appellant was convicted of an offense that was alleged in the charged specification. We affirm the judgment of the United States Navy-Marine Corps Court of Criminal Appeals (CCA).

I. Background

After becoming intoxicated during shore liberty, Appellant became embroiled in arguments with some shipmates. He cut and stabbed one and assaulted several who were trying to bring Appellant under control. Contrary to his pleas, Appellant was convicted by court members of willfully disobeying the order of a petty officer; wrongfully using provoking words; and various assaults, batteries, and aggravated assault. Articles 91, 117, and 128, UCMJ, 10 U.S.C. §§ 891, 917, 928 (2006). The convening

authority approved the adjudged sentence: a bad-conduct discharge, confinement for nine months, and reduction to the lowest enlisted grade. The CCA affirmed. United States v. Rauscher, No. 201000684, 2011 CCA LEXIS 165, at \*8-\*9, 2011 WL 4505922, at \*3 (N-M. Ct. Crim. App. Sept. 27, 2011).

## II. The Specification and Trial

A fundamental purpose of a specification is "to provide notice to an accused as to the matters against which he must defend." United States v. Wilkins, 29 M.J. 421, 424 (C.M.A. 1990); see Russell v. United States, 369 U.S. 749, 767 (1962). Appellant was charged with assault with intent to commit murder, a violation of Article 134, UCMJ, as follows:

In that [Appellant], on active duty, did, . . . on or about 29 March 2010, with the intent to commit murder, commit an assault upon Machinist's Mate Second Class Petty Officer [JD], U.S. Navy, by stabbing him in the hand and chest with a knife.

The military judge instructed the members on the offense of assault with intent to commit murder. At the request of both parties, the military judge also instructed the members on the offense of assault with a dangerous weapon or other means or force likely to produce death or grievous bodily harm, under Article 128, UCMJ, and that is what he was convicted of. The elements of that offense are:

- (i) That the accused attempted to do, offered to do, or did bodily harm to a certain person;

(ii) That the accused did so with a certain weapon, means, or force;

(iii) That the attempt, offer, or bodily harm was done with unlawful force or violence; and

(iv) That the weapon, means, or force was used in a manner likely to produce death or grievous bodily harm.

United States v. Dacus, 66 M.J. 235, 238 (C.A.A.F. 2008) (citing Manual for Courts-Martial, United States pt. IV, ¶ 54.b.(4)(a) (2005 ed.)).

Whether a specification states an offense is a question of law we review de novo. United States v. Crafter, 64 M.J. 209, 211 (C.A.A.F. 2006). Even if we assumed that the specification was defective in alleging an assault with intent to commit murder, we are convinced that the specification clearly alleges every element of the offense of assault with a dangerous weapon or means or force likely to produce death or grievous bodily harm, the offense he was convicted of:<sup>1</sup>

(1) Appellant did bodily harm to JD -- stabbing him in the hand and chest:

---

<sup>1</sup> In order to determine whether an indictment charges an offense against the United States, designation by the pleader of the statute under which he purported to lay the charge is immaterial. He may have conceived the charge under one statute which would not sustain the indictment but it may nevertheless come within the terms of another statute.

United States v. Hutcheson, 312 U.S. 219, 229 (1941).

(2) He did so with a certain weapon, means, or force -- a knife;

(3) The bodily harm was done with unlawful force or violence -- without authorization or justification; and

(4) The weapon, means, or force was used in a manner likely to produce death or grievous bodily harm -- stabbing JD in the chest.

The specification clearly placed Appellant on notice of that against which he had to defend. The Government's theory of the case from beginning to end was that Appellant stabbed the victim with a tactical knife in the hand and chest. Appellant defended against this theory throughout the trial. Appellant proposed instructions for the Article 128 offense and did not object to the instructions given by the military judge. In closing, defense counsel even asked the panel to "closely look" at Article 128 because "that's much more aligned with what happened." Through these actions, Appellant demonstrated that he was on notice, and his "substantial right to be tried only on charges presented in [a specification]" was not violated.

Stirone v. United States, 361 U.S. 212, 217 (1960).

IV.

The judgment of the United States Navy-Marine Corps Court of Criminal Appeals is affirmed.

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, [REDACTED]  
Headquarters and Headquarters Company,  
U.S. Army Garrison, Joint Base Myer-  
Henderson Hall, Fort Myer, VA 22211

)  
) **RULING: DEFENSE RENEWED**  
) **MOTION: DISMISS**  
) **SPECIFICATIONS 13 AND 14**  
) **OF CHARGE II - FAILURE**  
) **TO STATE AN OFFENSE**

) DATED: 18 July 2012  
)

Defense moves the Court for the second time to dismiss Specifications 13 and 14 of Charge II for failure to state an offense because the Government has failed to allege the Accused's conduct "exceeded authorized access" within the meaning of 18 U.S.C. Section 1030(a)(1). Government opposes. After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

**Factual Findings:**

1. The Court adheres to the facts as stated in the 8 June 2012 prior ruling on this issue.
2. The Court further finds that the Government proffers that for specification 13, the evidence will show that the accused "exceeded authorized access" when he obtained the relevant information using an unauthorized program, Wget.

**The Law: Failure to State an Offense.**

1. The military is a notice pleading jurisdiction. A charge and its specification is sufficient if it (1) contains the elements of the offense charged and fairly informs an accused of the charge against which he must defend; and (2) enables the accused to plead an acquittal or conviction in bar of future prosecutions for the same offense. In reviewing the adequacy of a specification, the analysis is limited to the language as it appears in the specification, which must expressly allege the elements of the offense or do so by necessary implication. *United States v. King*, 71 M.J. 50, fn 2, (C.A.A.F. 2012), quoting *United States v. Fosler*, 70 M.J. 225, 229 (C.A.A.F. 2011) and *United States v. Fleig*, 16 C.M.A. 444, 445 (1966) (looking "within the confines of the specification"). A motion to dismiss for failure to state an offense is a challenge to the adequacy of a specification and whether the specification "alleges, either expressly or by implication, every element of the offense, so as to give the accused notice and protection against double jeopardy." *United States v. Amazaki*, 67 M.J. 666, 669, 670 n.8 (A. Ct. Crim. App. 2009) (quoting *United States v. Crafter*, 64 M.J. 209, 211 (C.A.A.F. 2006)).

APPELLATE EXHIBIT 218  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

2. This Court has the power to dismiss charges before evidence is presented in accordance with Rule for Courts-Martial (R.C.M.) 907(b)(1) only when the issue is capable of resolution without trial on the issue of guilt.

**The Law: The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. Section 1030(a)(1).** The Court adheres to the law as stated in the 8 June 2012 ruling on this issue.

**Conclusions of Law:**

1. The language of Specifications 13 and 14 of Charge II includes all of the elements of the offense, fairly informs the accused of the charge against which he must defend, and protects the accused against double jeopardy. *See King*, at 51, n.2; *Fosler*, at 229; *Fleig*, at 445.

2. Although this Court has the power to dismiss a specification prior to trial when the issue is capable of resolution without trial on the issue of guilt, this power should be used sparingly. Unlike the cases presented to the Court, Specifications 13 and 14 of Charge II allege that the accused “exceeded authorized access” to classified information under 18 U.S.C. Section 1030(a)(1). Restrictions on access to classified information are not limited to code based or technical restrictions on access. Restrictions on access to classified information can arise from a variety of sources, to include regulations, user agreements, and command policies. Restrictions on access can include manner of access. User agreements can also contain restrictions on access as well as restrictions on use. The two are not mutually exclusive. The Court does not find that this issue is capable of resolution prior to presentation of the evidence. These issues are appropriately decided after the formal presentation of the evidence either as a motion for a finding of not guilty under R.C.M. 917 or a motion for a finding that the evidence is not legally sufficient. *King*, 71 M.J. 50; *United States v. Griffith*, 27 M.J. 42 (C.M.A. 1988).

3. The 1996 legislative history also evidences Congress’ intent that “exceeds authorized access” is not limited to code breaking restrictions on access. (18 U.S.C. Section 1030(a)(1) as amended “covers the conduct of a person who deliberately breaks into a computer without authority, or an insider who exceeds authorized access, and thereby obtains classified information and then communicates the information to another person, or retains it without delivering it to the proper authorities....It is the use of the computer that is being proscribed, not the unauthorized possession of, access to, or control over the information itself.”) S.Rep.No. 104-357, at 6 (1996).

4. The Court considered *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). *Drew* upheld a felony charge under 18 U.S.C. Section 1030(c)(2)(B)(ii) against challenges on grounds of vagueness, failure to state an offense, and unconstitutional delegation of powers finding that *scienter* element requiring the intentional accessing of a computer without authorization or in excess of authorization to be in furtherance of the commission of a crime or tortious act overcame the Constitutional challenges and arguments against criminalizing breaches of contract involving use of computers. Following acquittal on the felony offense, *Drew* held that basing a misdemeanor conviction under the Computer Fraud Act as per 18 U.S.C. Sections 1030(a)(2)(C) and 18 U.S.C. (e)(2)(A) upon the conscious violation of a website’s terms of service was void for vagueness. These lesser included misdemeanor offenses with no *scienter* requirement or a *scienter* requirement of only intent to access a computer without authorization or exceed

authorized access were void for vagueness because the misdemeanor statutes did not provide actual notice or minimal guidelines to govern law enforcement. The Court's earlier decision to uphold the felony charge in 18 U.S.C. Section 1030(c)(2)(B)(ii) is in accord with the broad view of the *United States v. Rodriguez*, 628 F.3d 1258 (11<sup>th</sup> Circuit 2010) line of cases.

5. In its 8 June 2012 ruling on the original motion to dismiss, the Court found the language in the statute and legislative history of the definition of "exceeds authorized access" ambiguous, applied the rule of lenity, and stated an intent to instruct in accordance with the narrow interpretation that "exceeds authorized access" is limited to violations of restrictions on *access* to information and not restrictions on the *use* of the information.

**RULING:** The Defense Renewed Motion to dismiss Specifications 13 and 14 of Charge II for failure to state an offense is **DENIED**. The Court will instruct in accordance with its 8 June 2012 ruling.

So **ORDERED**: this 18<sup>th</sup> day of July 2012.

A handwritten signature in black ink, appearing to read 'D R L', is written above the printed name.

DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

)  
)  
) **RULING: LESSER**  
) **INCLUDED OFFENSE**  
) **MAXIMUM**  
) **PUNISHMENTS**

) **DATED:** 19 July 2012  
)

The parties have presented the Court with their views of the maximum punishment for specification 1 of Charge II, and for the lesser included offense theories under clause 1 and 2 of Article 134 for the offenses charged under all 3 clauses of Article 134 (18 U.S.C. Section 641, 18 U.S.C. Section 793(e) and 18 U.S.C. 1030(a)(1)). After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

**The Law: Lesser Included Offense Maximum Punishment – Offenses Charged Under Clauses 1 and 2 of Article 134.**

1. For offenses not listed in Part IV of the Manual for Court-Martial (MCM), the maximum punishment depends on whether or not the offense is included in or closely related to a listed offense in the MCM. RCM 1003(c)(2)(B)(i).
2. A clause 1 and 2 offense not included in or closely related to a listed offense is punishable as authorized by the United States code or as authorized by the custom of the service. RCM 1003(c)(2)(B)(ii). Although there is authority that if an accused's misconduct cannot be charged under a listed offense, that listed offense cannot be a closely related offense (*U.S. v. Tenney*, 60 M.J. 838 (N.M.Ct. Crim. App. 2005)), there is contrary authority. See *U.S. v. Sampson*, 1 M.J. 266 (C.M.A. 1976) and *U.S. v. Hopkins*, 55 M.J. 546 (N.M. Ct. Crim. App. 2001 (a violation of 18 U.S.C. 1001(a) charged as a clause 1 and 2, Article 134, UCMJ offense is closely related to a violation of Article 107, UCMJ for sentencing purposes.)
3. Where the clause 1 and 2 specification lists every element of the act prohibited by the United States Code except the jurisdictional element, the maximum punishment may be the maximum punishment for the United States Code offense. *United States v. Leonard*, 64 M.J. 381 (C.A.A.F. 2007).
4. Where the clause 1 and 2 offense does not include the conduct and *mens rea* proscribed by a directly analogous federal criminal statutes or the offense is comprised of acts that cannot be criminally charged under the United States Code at all the offense is neither directly analogous nor essentially the same as a United States Code offense. *United States v. Beaty*, 70 M.J. 39 (C.A.A.F. 2011).
5. Clause 1 and 2 offenses not specifically listed in the MCM that are not closely related to or included in a listed offense, that do not describe acts that are criminal under the United States Code, and where there is no maximum punishment authorized by the custom of the service, are punishable as "general" or "simple" disorders with a maximum sentence of four months confinement, and forfeiture of two-thirds pay per month for 4 months. *Beaty*, 70 M.J. at 45.

APPELLATE EXHIBIT <sup>(219)</sup> CCXIX  
PAGE REFERENCED:  
PAGE 1 OF 2 PAGES



## Conclusions of Law.

1. Should the offenses charged under 18 U.S.C. Sections 641, 793(e), 1030(a)(1) and Article 134 be found by the fact-finder to be lesser included offenses under clause 1 and/or 2 of Article 134 without any additional change to the elements, the maximum penalty will be:

A. The clause 1 and 2 offenses charged using the elements of 18 U.S.C. Section 641 are closely related to Article 121, UCMJ, Larceny of Military Property of a value in excess of \$500.00 for specifications 4, 6, 8, and 16. The maximum penalty for that offense is 10 years confinement, a dishonorable discharge, and forfeiture of all pay and allowances for each specification. Specification 12 is closely related to Article 121, UCMJ, Larceny of Non-Military Property of a value in excess of \$500.00. The maximum penalty for this offense is 5 years confinement, a dishonorable discharge, and forfeiture of all pay and allowances.

B. The clause 1 and 2 offenses charged using the elements of 18 U.S.C. Section 793(e)/Article 134, UCMJ and 1030(a)(1)/Article 134, UCMJ are not closely related or included in any offense listed in part IV of the MCM. The clause 1 and 2 Article 134 offenses would be directly analogous to the respective United States Code offense per RCM 1003(c)(2)(B)(2)(ii). 18 U.S.C. Sections 793(e) and 1030(a)(1) each carry 10 years of confinement as a maximum sentence, thus the maximum penalty for each of specifications 2, 3, 5, 7, 9, 10, 11, 13, 14, and 15 of Charge II is 10 years confinement, a dishonorable discharge, and total forfeiture of all pay and allowances.

2. Specification 1 of Charge II is not closely related to any offense listed in part IV of the UCMJ, nor is it directly analogous to an offense under the United States Code. AR 380-5 dated 29 September 2000 (Information Security Program), does not penalize the conduct as charged in specification 1 of Charge II as a violation of Article 92, UCMJ, however, it does establish a custom of the service penalizing disclosures of classified and sensitive information. Disclosures charged under Article 92 would carry a maximum punishment of confinement for 2 years, a dishonorable discharge, and total forfeiture of all pay and allowances. This will be the maximum penalty for specification 1 of Charge II.

3. Should other lesser included offenses be raised by the evidence, the Court will address the maximum punishment for any such offenses after all of the evidence has been presented.

So **ORDERED**: this 19<sup>th</sup> day of July 2012.



DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**Prosecution Request  
for Leave until 17 August 2012  
to Provide Notice and Disclosure  
of Certain Documents**

**19 July 2012**

1. The United States requests leave of the Court until 17 August 2012 (1) to notify the Court with a status of whether it anticipates the custodian of classified evidence will seek limited disclosure IAW MRE 505(g)(2) or claim a privilege IAW MRE 505(c) for the classified information under that agency's control; (2) to file notice IAW MRE 505(i)(2), if necessary; and (3) if necessary, to disclose such files regarding the Accused that involve investigation, damage assessment, or mitigation measures to the Defense or, submit them to the Court for in camera review under RCM 701(g) or for limited disclosure under MRE 505(g)(2) for the following information maintained by military authorities: U.S. Cyber Command (CYBERCOM) information and Department of Defense (DoD) information classified collateral to "secret" and classified above the "secret" level or containing specialized control measures.

2. On 22 June 2012, in regard to "files under the possession of military authorities," the Court ordered, the following:

The Government will seek out and identify such files regarding PFC Manning that involve investigation, damage assessment, or mitigation measures. By 20 July 2012 the Government will notify the Court with a status of whether it anticipates any government entity that is the custodian of classified evidence that is the subject of the Defense Motion to Compel will seek limited disclosure IAW MRE 505(g)(2) or claim a privilege IAW MRE 505(c) for the classified information under that agency's control. Also by 25 July 2012, if the relevant agency claims a privilege under MRE 505(c) and the Government seeks an in camera proceeding under MRE 505(i), the Government will move for an in camera proceeding IAW MRE 505(i)(2) and (3) and provide notice to the Defense under MRE 505(i)(4)(A). For all such files where a privilege under MRE 505(c) is not claimed, by 3 August 2012 the Government will disclose such files regarding PFC Manning that involve investigation, damage assessment, or mitigation measures to the Defense or, submit them to the Court for in camera review under RCM 701 (g) or for limited disclosure under MRE 505(g)(2).

See Ruling: Defense Motion to Compel Discovery #2, dated 22 June 2012 (AE CXLVIII (147)). CYBERCOM "files" were not included in the Defense Motion to Compel.

3. The United States was first notified of the defense request for CYBERCOM investigative "files" on 23 June 2012, the day after the Court's ruling. The defense submitted to the Court a request for clarification and specifically named CYBERCOM "files" as being potentially being material to the preparation of defense. *See* Defense Request for Clarification of Court Ruling on Motion to Compel Discovery #2, dated 23 June 2012 (AE CLXXI (171)). The Court's clarification did not address CYBERCOM. *See* Ruling: Defense Motion-Clarification of Ruling Motion to Compel Discover 2, dated 25 June 2012 (AE CLXXVI (176)). On 27 June 2012, the defense emailed the prosecution, to ensure that the prosecution understood that the defense interpreted the Court's 22 June 2012 discovery ruling to include CYBERCOM "files."

4. Based on the defense's notice, the prosecution, on 3 July 2012, requested CYBERCOM produce documents for the prosecution's review. On 7 July 2012, the prosecution received the more than 3,000 CYBERCOM documents for review. During this week's motions hearing, the United States started its review and will complete its review this week, but requires additional time to acquire the authority to release any material related to the Court's order.

5. The United States also reviewed the additional DoD documents that were the subject of the Defense Motion to Compel and identified more than 11,000 documents which were subject to the Court's order. The United States anticipates receiving the approval for the vast majority of those documents to be disclosed to the defense by 3 August 2012. The United States requests additional time to obtain authorization to disclose a small portion of those documents that require additional review based on their classification and the original owning agency or department.

6. This request is in response to a defense request for more information. It will not necessitate a delay in the proceedings as the continued effort to obtain and release this information will occur concurrently with the scheduled pretrial motions process. There will be no prejudice to the defense.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

## UNITED STATES

**RULING: GOVERNMENT  
MOTION TO PRECLUDE  
REFERENCE TO ACTUAL  
HARM OR DAMAGE ON  
MERITS**

DATED: 19 July 2012

information; third, determine whether there are countermeasures to minimize or eliminate the damage to national security; and fourth, prepare the actual damage assessment.

6. A damage assessment measures, "given the nature of the information and the countermeasures, if any, that will be employed, the probable impact the compromise will have on our national security." Producing a damage assessment "is sometimes a long-term, multi-disciplinary analysis of the adverse effects of the compromise on systems, plans, operations, and/or intelligence."

#### **Reasons Government Moves to Preclude Mention of Actual Damage on the Merits**

1. Actual harm is not relevant to the charges facing the accused or to any available defense.

A. None of the charges require the government to prove actual damage, therefore actual damage is not relevant to any element of any offense for which the accused is charged.

B. Actual damage is not relevant to whether documents were classified or whether they relate to the national defense.

C. Actual damage is not relevant to any defense.

D. The evidence is not relevant to cross examine the OCA because classification reviews are forward thinking where the OCA determines whether the unauthorized disclosure of the information could reasonably be expected to result in damage to the national security. Use of damage assessments to impeach an OCA who prepared a classification review would be improper.

E. Challenges to the classification review conducted by the OCA are non-justiciable political questions. Classification reviews determine that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security. Damage assessments may be relevant to impeach an OCA, but only if the OCA authored the document and only with respect to the assessment, not the classification review under RCM 914.

2. Even if relevant, the evidence should be excluded under MRE 403 because the probative value of the actual damage would be outweighed by the danger of unfair prejudice, confusion of the issues, misleading the members, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence. Evidence of actual harm or lack thereof will create an undue tendency to lure fact finder into finding guilt or innocence irrespective of evidence supporting the charge.

#### **Defense proffered reasons the Court should deny the Government motion:**

1. The Government motion is overbroad in that it seeks to prevent the Defense from introducing any evidence related to actual harm or damage. Specific information in damage assessments could be relevant to whether the information was expected to cause harm

2. Actual damage is relevant to the 18 U.S.C. Section 793(e) and Section 1030(a)(1) offenses in that absence of actual harm is probative of whether the information leaked was of the type that the accused reasonably believed would cause harm.

3. Actual damage is relevant to the 18 U.S.C. Section 793(e) and Section 1030(a)(1) offenses in that absence of actual harm is probative of whether the accused had reason to believe that the information leaked could cause injury to the United States or to the advantage of any foreign nation.

4. Actual damage is relevant to specification 1 of Charge II in that lack of damage is probative of whether the accused acted wantonly.

5. Actual damage is relevant to the accused's defense that by virtue of his expertise and training, he knew which documents and information could be used to the injury of the United States or to the advantage of any foreign nation and selected only that information to release. Lack of damage corroborates the reasonableness of that belief.

6. Absence of damage is proper impeachment for OCA determinations that information could cause damage.

7. Absence of damage is proper to explore the bias of government agency witnesses who exaggerate potential damage.

#### **The Law.**

1. Military Rule of Evidence (MRE) 401 defines "Relevant Evidence". Relevant evidence means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more or less probable than it would be without the evidence. The military judge has the initial responsibility to determine whether evidence is relevant under RCM 401. *U.S. v. White*, 69 M.J. 236 (C.A.A.F. 2010).

2. MRE 402 provides that all relevant evidence is admissible, except as otherwise provided by the constitution of the United States as applied to members of the armed forces, the code, these rules, this Manual, or any Act of Congress applicable to members of the armed forces. Evidence which is not relevant is not admissible.

3. Relevant evidence is necessary when it is not cumulative and when it would contribute to a party's presentation of the case in some positive way in a matter at issue. A matter is not at issue when it is stipulated as fact (discussion to RCM 703(b)(1)).

4. MRE 403 provides that relevant evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the members, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.

5. The Sixth Amendment of the Constitution provides an accused the right to confront witnesses against him. That right includes cross examination and an opportunity to impeach witnesses. The right to cross examination is not absolute. Courts balance competing state interests inherent in rules limiting cross examination. *Chambers v. Mississippi*, 410 U.S. 284, 295 (1973); *Davis v. Alaska*, 415 U.S. 308, 316 (1974); *Crane v. Kentucky*, 476 U.S. 683, 690 (1986) (Judges retain wide latitude to impose reasonable limits on cross-examination based on concerns about, among other things, harassment, prejudice, confusion of the issues, witness safety, repetitive or irrelevant.)

## Conclusions of Law:

1. The 18 U.S.C. Section 793(e) and 1030(a) offenses require the Government to prove that at the time the accused allegedly disclosed the information in each of the relevant specifications, the accused had reason to believe the information he disclosed could be used to the injury of the United States or to the advantage of any foreign nation and that the accused acted willfully in that he made a conscious choice to communicate the covered information.
2. Specification 1 of Charge II requires the Government to prove the accused wrongfully and wantonly caused to be published on the internet intelligence belonging to the United States government, having knowledge that intelligence published on the internet is accessible to the enemy.
3. Whether actual harm or damage resulted is not an element of any of the charged offenses, nor is it probative of the whether the accused had reason to believe that the information leaked could be used to the injury of the United States or to the advantage of any foreign nation, nor is it probative of the accused's state of mind at the time of the commission of the alleged offenses.
4. The first five bases for the Defense relevance proffer for lack of actual damage all relate to the nature of the information disclosed and the accused's state of mind on or before the date(s) he disclosed the information. What, if any, actual damage occurred after disclosure of the information was not knowable to the accused at the time he disclosed the information. Thus, actual damage, or lack thereof, is not relevant to any of those five bases. The critical language is "reason to believe could be used." *U.S. v. Diaz*, 69 M.J. 127, 132 (C.A.A.F. 2010).
5. Similarly, the OCA classification determinations for the information allegedly disclosed by the accused were made on or before the dates of disclosure. Again, the relevant point of inquiry is the nature and classification status of the information on or before the date of disclosure. What, if any, future damage actually resulted was not knowable to the OCA at the time the OCA made the classification decision. Even if an OCA misjudged the information upon which it based its classification decision does not change the fact that the decision itself was made and communicated to the accused. Post-release damage or lack thereof is not relevant to impeach an OCA.
6. A secondary basis for excluding evidence of actual damage is under MRE 403. By allowing evidence of actual damage when the relevant inquiry is on the nature of the information allegedly disclosed on or before the disclosure, whether the accused had reason to believe the information could be used to the injury of the United States or to the advantage of any foreign nation on or before the date of disclosure, and the accused's *mens rea* on or before the date of disclosure, the members will be confused with the focus of the trial shifting to whether there was or was not actual damage and what, if any steps were taken by the Government to mitigate the damage.
7. The Court does not have sufficient information at this time to preclude the Defense from using evidence of actual damage to impeach a Government witness for bias. The Court defers ruling unless and until the issue ripens at trial.
8. The Court defers ruling on whether lack of actual harm or damage assists in presenting a viable defense. In order for the Court to appropriately rule on whether actual damage corroborates the reasonableness of the accused's belief, there must be some evidence that the accused knew the information could not be used to the injury of the United States or to the advantage of any foreign nation.

9. The Government motion to preclude the defense from raising or eliciting any discussion, reference, or argument, to include the introduction of documentary or testimonial evidence, relating to actual harm or damage from pretrial motions related to the merits portion of trial and from the merits portion of trial is overbroad. The Government motion to preclude the Defense from using evidence of actual damage during the merits portion of the trial is granted in part as set forth in the preceding paragraphs. This ruling does not preclude the Defense from using information in the damage assessments relevant to the nature of the information as it existed on or before the dates of the alleged disclosure of the information by the accused.

**RULING:** The Court finds that actual harm or damage is neither an element nor relevant to an element of these specifications. Accordingly, both the government and defense are precluded from introducing evidence of actual harm or damage during the merits portion of trial without prior approval of the Court. The Government Motion to Preclude Actual Harm or Damage from the Pretrial Motions Practice and the Merits Portion of Trial is **GRANTED IN PART**. This ruling does not affect the ability of either side to present actual harm evidence at sentencing.

So **ORDERED** this 19<sup>th</sup> day of July 2012.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit



UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**Ruling: Defense Motion to  
Compel Department of State  
Discovery – Motion to Compel #2**

**19 July 2012**

1. The Government has identified the following potentially discoverable information from the Department of State (DOS):

(1) The written assessments produced by the Chiefs of Mission used to formulate a portion of the draft damage assessment completed in August of 2011 consist largely of cables sent to, and from, affected embassies relating to the cables released up until August of 2011;

(2) The written Situational Reports produced by the WikiLeaks Working Group, a 24/7 working group composed of senior officials from throughout the Department designed to monitor the immediate crisis stemming from the released cables and coordinate the Department's response, between roughly 28 November 2010 and 17 December 2010, consist of the then real-time developments regarding cables released up until that time, summaries of published news articles relating to the cables released up until that time, and updates from select regions of the world regarding the cables released up until that time;

(3) The written minutes and agendas of meetings by the Mitigation Team, a group created to address the policy, legal, security, counterintelligence, and information assurance issues presented by the release of these documents, consist of formal meeting notes, PowerPoint slides of administrative matters and substantive issues, and documentation on information exchanged with other federal organizations;

(4) The Information Memoranda for the Secretary of State produced by WPAR, a group tasked with identifying persons referenced in released cables who are at risk, providing guidance to local embassies who request assistance on behalf of those persons, and tracking all persons at risk, consist of background information relating to the creation of the WPAR, any assistance requested by embassies from the WPAR (to include examples of requested assistance), regional reports by bureaus, guidance to embassies on how to identify and assist persons at risk, summaries of WPAR's duties, and the status of reviewed cables related to persons at risk;

(5) The matrices produced by WPAR consist of PII of individuals and their family members who are identified by WPAR as persons at risk based on the released cables to track the status of these individuals;<sup>1</sup>

<sup>1</sup> For the purpose of this Motion, the prosecution considers PII to include any information that could be used by another to identify a specific individual.

(6) The formal guidance produced by WPAR and provided to all embassies, including authorized actions for any identified person at risk consists of procedures for embassies seeking assistance from WPAR, the steps the Department takes should someone request relocation, additional options available to the embassies, and a list of best practices;

(7) The information collected by the Director of the Office of Counter Intelligence and Consular Support within the Department regarding any possible impact from the disclosure of diplomatic cables consists of translated foreign open-source internet articles, select cables, the Department's draft damage assessment dated August 2011 to which the defense already has access, regional assessments relating to the released cables, and no other versions of the draft assessment; and

(8) The Department did not find any prepared written statements for the Department's reporting to Congress on 7 and 9 December 2010. Based on those dates and Under Secretary Kennedy's testimony, only informal discussions would have occurred between Department officials and members of Congress, therefore there are no written statements or other documents.

2. The volume of records gathered is more than 5,000 documents and most are classified. In light of the volume of documents and interagency coordination involved, the Government requests 45-60 days to review the documents and determine whether to seek limited disclosure or claim a privilege. The Defense opposes.

3. The Government has advised the Court of its intent in its sentencing case to introduce evidence of actual harm and impact to the DOS regarding each of the above categories except (3) and (8) (which evidence the Government asserts does not exist).

4. The Court has previously ordered disclosure of the interim damage assessment prepared by the Department of State to the Defense.

5. The Government moves the Court to deny the Defense Motion to Compel the following information on the grounds that they are not relevant and necessary and for category (1) that it is cumulative.

(1) Information that predated, and contributed to, the Department of State draft damage assessment dated August 2011;

(2) Purely administrative records; and

(3) Personally Identifiable Information (PII) of persons negatively affected by the unauthorized disclosures, to include those persons identified by the WikiLeaks Persons at Risk Group (WPAR) as being put at risk.

6. Defense moves for the Court to order all DOS information not disclosed to the Defense to be disclosed to the Court for *in camera* review and for the Court to order that for all remaining discovery, the Government order the Court to consult with equity holders simultaneously.

7. Defense has advised the Court that it has evidence of alleged people at risk coming forward publicly to state they were not at risk. The Defense provided a newspaper article to the Court today.

### **The Law.**

The Court adopts the law as set forth in its 23 March 2012 and 22 June 2012 rulings on discovery issues.

### **Conclusions of Law.**

1. The Government shall search all of the above information for material required to be disclosed to the defense that is material and favorable to the defense under *Brady v. Maryland*, 373 U.S. 83 (1963).
2. The Government is presenting evidence in sentencing aggravation, to include expert opinion testimony, of the damage to the Department of State, foreign relations, and national security because by the accused's alleged disclosures. Information that forms the basis of the sentence aggravation and for an expert opinion is material to the preparation of the defense and relevant and necessary to be produced under RCM 703(f) for discovery. Aggravating information that the Government will not use or reference during sentencing or that does not form the basis of a government witness' opinion is not material to the preparation of the defense or relevant and necessary for discovery.
3. The underlying raw data forming the basis for the damage assessment is not cumulative for discovery purposes. It is material to the preparation of the defense and relevant and necessary to be produced for discovery under RCM 703(f).
4. The Government has advised the Court it will not present any evidence in sentencing regarding the Mitigation Team. As such, the Government is required only to disclose *Brady* material from this information to the Defense.
5. The Court grants the Government's motion to exclude purely administrative records and records that are not relevant to this case. The Government will produce and disclose any records of the timing of relevant group meetings and how long the meetings lasted.
6. The Government motion to exclude the PII of persons negatively affected by the accused's alleged disclosures is granted except that the Government will disclose the PII of any persons identified in the newspaper article the Defense presented to the Court that is maintained by the DOS as persons negatively affected. The Defense has not presented evidence to the Court that any additional PII information is relevant and necessary for discovery.
7. The Defense motion to require the Government to provide the Defense with all discovery or to give all information not disclosed to the Court for *in camera* review is denied.

**RULING:** The Defense motion to Compel Discovery #2 of State Department information is **GRANTED IN PART** as set forth above.

By **14 September 2012** the Government will disclose all discoverable information set forth above to the Defense, submit the discoverable information to the Court for *in camera review* as limited disclosure under MRE 505(g)(2), or advise the Court if DOS claims a privilege under MRE 505(c) and provide notice to the Court and the Defense whether the Government seeks an *in camera* proceeding under MRE 505(i).

**SO ORDERED:** this 19<sup>th</sup> day of July, 2012.

A handwritten signature in black ink, appearing to read 'DRL' followed by a stylized flourish.

DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

Modern Revised  
Jury Instructions  
CRIMINAL

SAND • GIFFORD • LOUGHEE  
REISS • ALLEN • RAKOFF

# *Publication Table of Contents*

## **MODERN FEDERAL JURY INSTRUCTIONS**

---

### **VOLUME 1**

---

#### **PART I GENERAL INSTRUCTIONS**

Chapter 1	Introduction
Chapter 2	The Function of the Court, the Jury and Counsel
Chapter 3	The Indictment, Statute and Charges
Chapter 3A	Scienter
Chapter 4	Burden of Proof
Chapter 5	Evidence
Chapter 6	Inferences
Chapter 7	Witness Credibility
Chapter 8	Defenses
Chapter 9	Concluding General Instructions
Chapter 9A	Federal Death Penalty

---

#### **PART II SUBSTANTIVE INSTRUCTIONS**

Chapter 10	Attempt
Chapter 11	Aiding and Abetting (18 U.S.C. §§ 2(a), 2(b))
Chapter 12	Accessory After the Fact (18 U.S.C. §§ 3, 4)
Chapter 13	Air Piracy
Chapter 14	Assault Upon a Federal Officer (18 U.S.C. §§ 111, 115)
Chapter 15	Bankruptcy Fraud (18 U.S.C. §§ 152, 157)
Chapter 16	Bribery of Public Officials (18 U.S.C. §§ 201, 215)
Chapter 16A	Failure To Pay Child Support (18 U.S.C. § 228)
Chapter 17	Civil Rights
Chapter 18	False Claims Against the Government (18 U.S.C. § 287)
Chapter 19	Conspiracy (18 U.S.C. § 371)
Chapter 19A	Solicitation To Commit a Crime of Violence (18 U.S.C. § 373)
Chapter 20	Contempt (18 U.S.C. § 401)
Chapter 21	Counterfeiting (18 U.S.C. §§ 471-473)
Chapter 22	Forgery (18 U.S.C. §§ 495, 510, 513)
Chapter 23	Smuggling (18 U.S.C. § 545)

Chapter 23A	Theft of Government Property (18 U.S.C. § 641)
Chapter 24	Embezzlement From Banks and Insurers (18 U.S.C. § 656)
Chapter 25	Theft From Interstate Shipment (18 U.S.C. § 659)
Chapter 26	Embezzlement From a Common Carrier (18 U.S.C. § 660)
Chapter 27	Theft From Employee Benefit Plans (18 U.S.C. § 664)
Chapter 27A	Federal Program Theft and Bribery (18 U.S.C. § 666; 7 U.S.C. § 2024)
Chapter 28	Escape From Custody (18 U.S.C. §§ 751, 752)
Chapter 29	Espionage (18 U.S.C. § 793)

## VOLUME 2

Chapter 30	Explosive Destruction of Property (18 U.S.C. § 844)
Chapter 31	Threatening Communications (18 U.S.C. §§ 871, 875, 876)
Chapter 32	Extortionate Credit Transactions (18 U.S.C. §§ 892, 894)
Chapter 33	False Claim of Citizenship (18 U.S.C. § 911)
Chapter 33A	Immigration Offenses (18 U.S.C. §§ 1324, 1326)
Chapter 34	False Personation (18 U.S.C. §§ 912-914)
Chapter 35	Firearms (18 U.S.C. §§ 922, 924; 26 U.S.C. § 5861)
Chapter 36	False Statements (18 U.S.C. § 1001)
Chapter 37	Bank Fraud (18 U.S.C. §§ 1005, 1010, 1014)
Chapter 38	Fugitives From Justice (18 U.S.C. §§ 1071-1073)
Chapter 39	Gambling (18 U.S.C. §§ 1082, 1084, 1953, 1955)
Chapter 39A	False Identification Documents (18 U.S.C. § 1028)
Chapter 40	Credit Card Fraud (18 U.S.C. § 1029)
Chapter 40A	Computer Fraud (18 U.S.C. § 1030)
Chapter 41	Homicide (18 U.S.C. §§ 1111, 1112, 1114, 1116)
Chapter 42	Kidnapping (18 U.S.C. §§ 1201, 1203, 1204)
Chapter 43	[Reserved]
Chapter 44	Mail, Wire, Bank and Health Care Fraud (18 U.S.C. §§ 1341, 1343, 1344)
Chapter 45	Obscenity (18 U.S.C. §§ 1461, 1462, 1464, 1465)
Chapter 46	Obstruction of Justice (18 U.S.C. §§ 1503, 1505, 1510-1513)
Chapter 47	Visa and Passport Fraud (18 U.S.C. §§ 1542, 1546)
Chapter 48	Perjury (18 U.S.C. §§ 1621-1623)
Chapter 49	Obstructing Correspondence (18 U.S.C. §§ 1702, 1708, 1709, 1711)

---

## VOLUME 3

Chapter 50	The Hobbs Act (18 U.S.C. § 1951)
Chapter 50A	Money Laundering (18 U.S.C. §§ 1956, 1957)
Chapter 50B	Records and Reports of Currency Transactions (31 U.S.C. §§ 5313, 5314, 5316, 5324)
Chapter 51	Criminal Labor Law Violations (18 U.S.C. § 1954; 29 U.S.C. § 186)
Chapter 52	RICO (18 U.S.C. §§ 1962, 1963)
Chapter 53	Bank Robbery (18 U.S.C. § 2113)
Chapter 53A	Carjacking (18 U.S.C. § 2119)
Chapter 54	Stolen Property (18 U.S.C. §§ 2312–2315)
Chapter 54A	Trademark and Copyright Offenses
Chapter 55	Bail Jumping (18 U.S.C. § 3146)
Chapter 56	Possession and Distribution of Controlled Substances (21 U.S.C. §§ 841, 843, 848; 21 U.S.C. §§ 856, 952)
Chapter 57	Securities Fraud (15 U.S.C. §§ 77–78)
Chapter 58	Criminal Antitrust Violations (15 U.S.C. § 2; 35 U.S.C. § 154)
Chapter 59	Tax Fraud (26 U.S.C. §§ 7201, 7203, 7206, 7212)
Chapter 60	The Travel Act (18 U.S.C. §§ 1952, 1958)
Chapter 61	Sexual Abuse (18 U.S.C. §§ 2241–2244)
Chapter 62	Child Pornography (18 U.S.C. §§ 2251, 2252, 2252A)
Chapter 63	Interstate Domestic Violence and Stalking (18 U.S.C. §§ 2261, 2261A)
Chapter 64	The Mann Act (18 U.S.C. §§ 2421–2423)
Chapters 65–70	[Reserved]
Table of Cases	
Table of Statutes	
Index	

---

## VOLUME 4

---

### PART III GENERAL CIVIL INSTRUCTIONS

Chapter 71	Function of the Court, the Jury and Counsel
Chapter 72	Corporations and Corporate Liability
Chapter 73	Burden of Proof
Chapter 74	Evidence
Chapter 75	Inferences and Presumptions



Chapter 76	Witness Credibility
Chapter 77	Damages
Chapter 78	Jury Deliberations

---

#### **PART IV SUBSTANTIVE CIVIL INSTRUCTIONS**

Chapter 79	Restraint of Trade (15 U.S.C. § 1)
Chapter 80	Monopolization (15 U.S.C. § 2)
Chapter 81	Patent Based Antitrust Claims (35 U.S.C. § 154)
Chapter 82	Securities-The 1934 Act (15 U.S.C. § 78)
Chapter 83	Securities-The 1933 Act (15 U.S.C. § 77)
Chapter 84	Civil RICO (18 U.S.C. § 1962)
Chapter 85	[Reserved]

---

#### **VOLUME 5**

Chapter 86	Patents
Chapter 86A	Trademark
Chapter 86B	Copyright
Chapter 87	Civil Rights Actions and the Fair Housing Act (42 U.S.C. §§ 1981-1985, 3604)
Chapter 88	Civil Rights Actions-Equal Pay Act and Age Discrimination in Employment Act; Jury Trial in Employment Discrimination Cases (29 U.S.C. §§ 206, 621, 623)
Chapter 88A	Americans with Disabilities Act
Chapter 89	Federal Employer's Liability Act (45 U.S.C. §§ 1, 23, 51)
Chapter 90	The Jones Act (46 U.S.C. § 688)
Chapter 91	Libel
Table of Cases	
Table of Statutes	
Index	

---

#### **VOLUME [★] PATTERN JURY INSTRUCTIONS (Criminal Cases)**

Pattern Criminal Jury Instructions for the District Courts of the First Circuit
Pattern Criminal Jury Instructions for the Third Circuit
Pattern Criminal Jury Instructions for the Fifth Circuit
Pattern Criminal Jury Instructions for the Sixth Circuit
Pattern Criminal Federal Jury Instructions for the Seventh Circuit

Manual of Model Criminal Jury Instructions for the District Courts of the Eighth Circuit

---

**VOLUME [ ★ ★ ] PATTERN JURY INSTRUCTIONS (Criminal Cases)**

Manual of Model Criminal Jury Instructions for the Ninth Circuit

Tenth Circuit Criminal Pattern Jury Instructions

Eleventh Circuit Pattern Jury Instructions

Federal Judicial Center, Pattern Criminal Jury Instructions

---

**VOLUME [ ◇ ] PATTERN JURY INSTRUCTIONS (Civil Cases)**

Fifth Circuit Pattern Jury Instructions (Civil Cases)

Seventh Circuit Pattern Jury Instructions (Civil Cases)

Manual of Model Civil Jury Instructions for the District Courts of the Eighth Circuit

Manual of Model Jury Instructions for the Ninth Circuit (Civil)

Eleventh Circuit Pattern Jury Instructions (Civil Cases)

Model Pattern Bankruptcy Jury Instructions (Civil Cases)

# MODERN FEDERAL JURY INSTRUCTIONS

---

## Volume 1

CRIMINAL

HON. LEONARD B. SAND

JOHN S. SIFFERT

WALTER P. LOUGHLIN

STEVEN A. REISS

STEVEN W. ALLEN

HON. JED S. RAKOFF

Cite as: 1 L. Sand, *et al.*, *Modern Federal Jury Instructions—Criminal*

2008

*Filed Through:*

RELEASE NO. 53B November 2008



LexisNexis®

# MODERN FEDERAL JURY INSTRUCTIONS

---

## Volume 2

CRIMINAL

HON. LEONARD B. SAND

JOHN S. SIFFERT

WALTER P. LOUGHLIN

STEVEN A. REISS

STEVEN W. ALLEN

HON. JED S. RAKOFF

Cite as: 2 L. Sand, *et al.*, *Modern Federal Jury Instructions—Criminal*

2008

*Filed Through:*

RELEASE NO. 53B November 2008



LexisNexis®

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Scheduling  
Order

DATE

1. The Court is currently scheduling Article 39(a) sessions with the following default schedule at the request of the parties: two weeks for parties to file motions; two weeks for parties to file responses; five days for parties to file replies; and one week for the Court to review all pleadings before the start of the motions hearing. The time for filing replies was added after the first Article 39(a) session on 15-16 March 2012 because the Court received reply briefs the day before that session, the parties desire to continue to file replies, and the Court requires time to consider them.

2. Scheduling dates and suspense dates are set forth below. This schedule was coordinated with the parties. The trial schedule will be reviewed and updated as necessary at each scheduled Article 39(a) session.

- a. Immediate Action (21 February 2012 - 16 March 2012)
- b. Legal Motions, excluding Evidentiary Issues (29 March 2012 - 26 April 2012)
- c. Legal Motions (10 May 2012 - 8 June 2012)
- d. Interim Pretrial Motions (2 June 2012 - 25 June 2012)
- e. Pretrial Motions (7 June 2012 - 20 July 2012)
- f. Pretrial Motions (20 July 2012 - 30 August 2012)

- (A) Filing: 3 August 2012
- (B) Response: 17 August 2012
- (C) Reply: 22 August 2012
- (D) Article 39(a): 28-30 August 2012

(1) **Defense Article 13 Motion**

- (A) Filing: 27 July 2012<sup>1</sup>
- (B) Response: 17 August 2012
- (C) Reply: 22 August 2012
- (D) Article 39(a): 1-5 October 2012<sup>2</sup>

<sup>1</sup> The defense agreed to the filing date of one week earlier to give the prosecution the necessary time to respond.

<sup>2</sup> This is also documented below in g(1).

- (2) **Government Witness List for Response to Defense Article 13 Motion**  
(A) Filing: 14 August 2012
- (3) **Defense Supplemental Request for Article 13 Witnesses**  
(A) Filing: 15 August 2012  
(B) Response: 22 August 2012  
(C) Reply: 24 August 2012
- (4) **Government Supplement to Request for Leave until 14 September 2012**<sup>3</sup>  
(A) Filing: 31 July 2012
- (5) **Motions in Limine**
- (6) **Motions to Suppress (if any)**
- (7) **Due Diligence Ex Parte Filing**  
(A) Filing: 25 July 2012
- (8) **Notification to the Court of Anticipated Limited Disclosures under MRE 505(g)(2) or Notification to the Court of Privilege under MRE 505(c) for Files under the Possession Custody, or Control of Military Authorities based on the Court's 22 June 2012 Ruling**  
(A) Filing: 20 July 2012
- (9) **Notification to the Court of Anticipated Limited Disclosures under MRE 505(g)(2) or Notification to the Court of Privilege under MRE 505(c) for FBI Investigative File based on the Court's 22 June 2012 Ruling**  
(A) Filing: 25 July 2012
- (10) **Government Filing for In Camera Proceeding IAW MRE 505(i) with Notice to Defense (if Privilege is Claimed) based on the Court's 22 June 2012 Ruling**  
(A) Filing: 25 July 2012
- (11) **Disclosure to Defense or Disclosure to the Court under RCM 701(g)(2) or MRE 505(g)(2) of All Information Subject to the Court's 22 June 2012 Ruling**<sup>4</sup>

---

<sup>3</sup> On 25 July 2012, the prosecution requested leave until 14 September 2012 to disclose a subset group of information owned by the Central Intelligence Agency (CIA), the Department of Homeland Security (DHS), and the Office of the Director of National Intelligence (ODNI). On 26 July 2012, the defense filed an objection. On 26 July 2012, the Court ordered the prosecution to file a supplemental pleading, stating with particularity the review and approval procedures required prior to disclosure of information above the "secret" level and how that differs from the review and approval procedures required prior to disclosure of information at or below the "secret" level.

<sup>4</sup> This disclosure includes all files that involve investigation, damage assessment, or military measures that are under the possession, custody, or control of military authorities; all FBI files that involve investigation, damage assessment, or mitigation measures; the ODNI/ONCIX damage assessment; and evidence the prosecution will introduce on the merits and during sentencing.

(A) Filing: 3 August 2012

**(12) Disclosure of All Remaining Unclassified or Classified (under MRE 505(g)(1))  
Brady Material and Disclosure under MRE 701(g)(2) or MRE 505(g)(2) of All Remaining  
Classified Brady Material<sup>5</sup>**

(A) Filing: 3 August 2012

**(13) Defense Witness List for Speedy Trial, including Article 10**

- (A) Witness Lists: 10 August 2012<sup>6</sup>
- (B) Government Objections (if any): 17 August 2012
- (C) Defense Motion to Compel (if any): 22 August 2012

**(14) Defense 505(h)(3) Notice for Damage Assessments and Other Classified  
Information Provided on 3 August 2012<sup>7</sup>**

- (A) Filing: 17 August 2012
- (B) Response: 22 August 2012

**(15) Disclosure to Defense, Disclosure to the Court under MRE 505(g)(2), Notification  
to the Court of Claim of Privilege under MRE 505(c), or Filing for *In Camera* Proceeding  
IAW MRE 505(i) with Notice to Defense (if Privilege is Claimed) for CYBERCOM  
Information and DoD Information Classified Above Secret or Containing Specialized  
Control Measures**

(A) Date: 17 August 2012

**(16) Preliminary Determinations on Admissibility #2**

**(17) Initial Requests for Judicial Notice**

**(18) RCM 914 Notification and Motions**

(A) Government Notification to Defense of Types of Information the Government  
Intends to Disclose to the Defense IAW RCM 914: 3 August 2012

---

<sup>5</sup> This production includes any material discovered while searching the files, if any, of the President's Intelligence Advisory Board, and all material that is not subject to Motions to Compel Discovery or Production. If the Court rules that any of the proposed summaries under MRE 505(g)(2) are not acceptable, the prosecution has advised that they may need additional time to obtain approval for a different substitution.

<sup>6</sup> On 23 July 2012, the prosecution and the defense agreed to 10 August 2012 in lieu of the 3 August 2012 date that was discussed in the RCM 802 conference. The defense also agreed not to object to a prosecution request for additional time to prepare its response if the prosecution cannot make contact with all the defense witnesses to respond by 17 August 2012.

<sup>7</sup> This notice is for all material that the prosecution produced to the Defense by 3 August 2012. If the Government proposes summaries that are not acceptable to the Court, and additional time is needed, the Defense will file a supplemental 505(h)(3) notice seven days after receiving the Court approved summaries under M.R.E. 505(g)(2). The required notice must be made in accordance with the Court's Protective Order for Classified Information, dated 16 March 2012. *See* AE XXXII, para. 3(l).

- (B) Defense Motion if Object to Scope of Government Notice: 17 August 2012
- (C) Government Reply: 22 August 2012

**(19) Updated Proposed Case Calendar**

- (A) Filing: 17 August 2012

**g. Interim Pretrial Motions (24 August 2012 - 5 October 2012)**

- (A) Article 39(a): 1-5 October 2012

**(1) Defense Article 13 Motion<sup>8</sup>**

- (A) Filing: 27 July 2012
- (B) Response: 17 August 2012
- (C) Reply: 22 August 2012

**(2) Defense Supplemental Article 13 Motion**

- (A) Filing: 24 August 2012
- (B) Response: 7 September 2012
- (C) Reply: 14 September 2012

**(3) Government Supplemental Article 13 Motion Witness List (if necessary)**

- (A) Filing: 4 September 2012

**(4) Court Member Questionnaires**

- (A) To Detailed Members and Alternates: 4 September 2012
- (B) Suspense for Detailed Members and Alternates to Respond: 21 September 2012

**(5) Defense Motion to Compel Discovery #3 (if necessary)<sup>9</sup>**

**(6) Disclosure to Defense, Disclosure to the Court under MRE 505(g)(2), Notification to the Court of Claim of Privilege under MRE 505(c), or Filing for *In Camera* Proceeding IAW MRE 505(i) with Notice to Defense (if Privilege is Claimed) for DOS Information Subject to the Court's 19 July 2012 Order**

- (A) Date: 14 September 2012

**h. Pretrial Motions (26 September 2012 - 2 November 2012)**

- (A) Filing: 28 September 2012
- (B) Response: 12 October 2012

---

<sup>8</sup> This motion is listed above in 2f because of the filing dates, but it will be litigated during the 1-5 October 2012 Article 39(a).

<sup>9</sup> The defense filed a discovery request with the prosecution on 19 July 2012 for information classified above the secret level. If necessary, litigation is tentatively scheduled for the Interim Pretrial Motions session. No filing dates are given at this point because they are contingent upon the prosecution's response to the defense discovery request and whether or not the defense files a motion to compel discovery.



- (C) Reply: 19 October 2012
- (D) Article 39(a): 29 October 2012-2 November 2012

**(1) Defense Motion for Speedy Trial, including Article 10<sup>10</sup>**

- (A) Filing: 26 September 2012
- (B) Response: 16 October 2012
- (C) Reply: 22 October 2012

**(2) Government Witness List for Response to Defense Motion for Speedy Trial, including Article 10**

- (A) Filing: 9 October 2012

**(3) Defense Notice of Intent to Disclose Classified Information under MRE 505(h) (From Subsequent Disclosures)**

- (A) Filing: 15 October 2012
- (B) Response: 26 October 2012

**(4) Witness List (Defense and Supplemental Government)**

- (A) Filing: 15 October 2012

**(5) Defense Production of Government Reciprocal Discovery Request**

- (A) Date: 15 October 2012

**(6) Defense Notice of Accused's Forum Selection and Notice of Pleas in Writing<sup>11</sup>**

- (A) Filing: 15 October 2012

**(7) Defense Notice of its Intent to Offer the Defense of Lack of Mental Responsibility IAW RCM 701(b)(2)**

- (A) Filing: 15 October 2012

**(8) Disclosure of RCM 914 Material**

- (A) Date: 15 October 2012

**i. Interim Pretrial Motions (26 November 2012)**

**j. Pretrial Motions (16 November 2012 - 14 December 2012)**

- (A) Filing: 16 November 2012
- (B) Response: 30 November 2012
- (C) Reply: 5 December 2012

---

<sup>10</sup> On 30 July 2012, the parties agreed to the modified dates to give both parties sufficient time to prepare their filings and the Court sufficient time to review the filings.

<sup>11</sup> If the accused selects a panel, the prosecution has requested that the panel be notified no less than sixty days prior to trial, in order to coordinate for extended special duty and travel.

(C) Article 39(a): 10-14 December 2012

(1) **Defense Witness List Litigation**

(A) Government Objection to Defense Witnesses: 16 November 2012

(B) Motion to Compel Production: 30 November 2012

(C) Response: 5 December 2012

(2) **Government Motion to Compel Discovery (if any)**

(3) **Additional Requests for Judicial Notice**

(4) **Pre-Qualification of Experts**<sup>12</sup>

(5) **Motions *in Limine* (Supplemental, Including any Classified Information) (if necessary)**

**k. Pretrial Motions (7 December 2012 - 18 January 2013)**

(A) Filing: 21 December 2012

(B) Response: 4 January 2013

(C) Reply: 9 January 2013

(D) Article 39(a): 14-18 January 2013

(1) **Litigation Concerning MRE 505(h) and MRE 505(i)**<sup>13</sup>

(A) Filing: 7 December 2012

(B) Response: 21 December 2012<sup>14</sup>

(2) **Supplemental Government Witness List**<sup>15</sup> (if necessary)

(A) Date: 14 December 2012

**(3) Production of Compelled Discovery from Government Motion to Compel Discovery**

(A) Date: 14 December 2012

---

<sup>12</sup> If the defense needs additional time to prequalify any contested experts based on the witness determinations, the defense can prequalify those experts at the 14-18 January 2013 Article 39(a).

<sup>13</sup> This includes *in camera* proceedings for Defense Notice to Disclose Classified Information and/or the Government's Invocation of the Privilege for Merits and Sentencing Information. The prosecution advised that any Court order to disclose classified information will likely require coordination with multiple federal organizations and roughly estimates forty-five to sixty days to coordinate a response across all equity holders.

<sup>14</sup> The adjusted date gives the Court additional time to review any discoverable material and was agreed to by the defense. The prosecution estimates the review will take no more than fifteen duty days to complete.

<sup>15</sup> The prosecution will submit a supplemental witness list based solely on any ruling from the Government Motion to Compel Discovery and any disclosures by the defense after the 15 October 2012 witness list due date.

(4) **Grunden Hearing for Government Classified Information**

(5) **Voir Dire Questions, Flyer, Findings/Sentence Worksheet, All CMCOs**  
(A) Filing for Court Review: 4 January 2013

**l. Pretrial Motions (28-29 January 2013)**

(1) **Grunden Hearing for Defense Classified Information**

(2) **Completion of Security Clearance Checks for Witnesses (as necessary)**

**m. Trial by Members (30 January 2013 - 22 February 2013)**

(1) **Voir Dire: 30 January 2013-31 January 2013**

(2) **Trial: 4-22 February 2013**

So **Ordered** this \_\_\_\_ day of \_\_\_\_\_ 2012.

DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, [REDACTED]  
Headquarters and Headquarters Company, U.S.  
Army Garrison, Joint Base Myer-Henderson Hall,  
Fort Myer, VA 22211

DEFENSE RESPONSE TO  
PROSECUTION PROPOSED  
CASE CALENDAR

DATED: 26 July 2012

RELIEF SOUGHT

1. PFC Bradley Manning, by and through the undersigned Defense counsel, opposes portions of the Government's proposed case calendar. The Defense requests that the Court amend the case calendar to reflect the issues noted by the Defense below.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Government has the burden of persuasion. RCM 905(c)(2)(A). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

3. On 19 July 2012, the Court and the parties participated in an 802 session to discuss the case calendar. During that discussion, the parties went through the proposed calendar. The Court directed the Government to capture the discussion into a revised proposed case calendar for review by the Court and the Defense.

4. On 25 July 2012, the Government submitted a case calendar to the Court. The Government's proposal was in the form of a Scheduling Order for the Court to sign.

ARGUMENT

5. The Defense objects to various aspects of the Government's proposed case calendar. Further, the Defense does not understand why this has been drafted in the form of a Scheduling Order and presented as though it represents consensus on all issues.

225  
PAGE 1 OF 1  
PAGE 1 OF 1 PAGES

6. The Defense has the following problems with the Government's proposed calendar:

- a) **Jencks:** The Government indicates that "Interpretation of Jencks" motions will be filed on 3 August 2012. The Defense did not agree to this filing date. The Government was the party that raised the possible *Jencks* issue. As such, the Government should be required to file a motion detailing its interpretation of *Jencks*, to which the Defense can respond. How can the Defense be expected to guess at what *Jencks* issues the Government sees and then address them? If the Government were not adopting an unorthodox view of *Jencks*, then it would not have felt the need to raise the issue for the Court. As such, it is incumbent on the Government to file a motion on the issue, not the Defense.
- b) **Motion to Compel Discovery #3:** The Government proposes that the Defense file a Motion to Compel Discovery #3, if necessary, at some point in advance of the 26 September interim motions argument. Given the Government's two separate requests for extensions of time until 14 September 2012 to produce discovery from the DOS, CIA, DHS and ODNI (or set the process in motion to claim a privilege), scheduling this motion for 26 September 2012 is untimely. The Defense needs to have the discovery in order to move to compel any additional discovery. This cannot be done in time for the 26 September 2010 interim hearing.
- c) **Latest Defense Discovery Request:** The Government notes in footnote 9 that the Defense has requested discovery stemming from one of the damage assessments. The Government has not indicated a proposed response date. It simply states, "any dates, however, are contingent upon the government's response to the defense discovery request and whether or not the defense files a motion to compel discovery." The due date for the Government's response should be placed on the case calendar. And, in any event, the due date should be well before whatever date is schedule for the Defense Motion to Compel Discovery #3.
- d) **Speedy Trial Motion:** Depending on the Court's ruling with respect to the Government's request for additional time to provide discovery, the Defense will likely move to reschedule the speedy trial motion such that it is litigated *after* discovery issues are complete.
- e) **505 Notice Issues:**
  - i) **August 3 Disclosures:** The Government proposes that the Defense give MRE 505 notice on 17 August for damage assessments and other classified information provided on 3 August. The Defense will do its best to adhere to the 17 August timeline (bearing in mind that Mr. Coombs is out of country until 10 August and that the Government has not yet approved military counsel to have full access to classified information). If there are limitations placed upon access (e.g. the classified information must be viewed in person), then the Defense will provide notice after having the opportunity to review the information, most likely after the August Article 39(a) session. For future 505(h) notices (e.g. the Government's proposed 505(h)

notice on 15 October), the Defense proposes providing the required notice within 30 days of receiving access to the information from the Government.

- ii) **505 Notice for Approved Summaries:** The Defense objects to providing 505 Notice within 7 days of receiving the Court-approved summaries. The Defense is not sure what limitations the Government may place on receiving these summaries (e.g. having to see them in person in the Washington D.C. areas; having to see them in the presence of security experts, etc.). Moreover, even if the Government were to provide the summaries to the Court-approved facility in Rhode Island, this usually requires coordinating in advance with the Naval War College, and allocating an entire day at the facility. Seven days is not a reasonable amount of turn-around time for the Defense. The Defense is particularly disappointed that the Government would attempt to force the Defense to respond within a week when the Government itself thinks nothing of requesting an additional two to three *months* to respond to virtually any issue.
- iii) **Rolling 505(h) Notice:** The Defense proposes providing the required notice within 30 days of receiving the information. The Government would then provide a response within 10-14 days (the Defense bases this off of the Government's own timeline at p. 4 where it indicates a filing date of 15 October and a Response date of 26 October). The issue would then be litigated at the subsequent Article 39(a) session.
- iv) **The Government's Interpretation of the Protective Order:** Further, the Defense believes that the Government's use of the phrase "The required notice must be made in accordance with the Court's Protective Order for Classified Information" at footnote 7 is intended to surreptitiously re-raise the issue of whether the Defense is obligated to disclose the names of the witnesses from whom the Defense will be eliciting the classified information on direct or cross-examination. The 505(h) notice does not require this disclosure, except to the extent that the Defense is eliciting this testimony through a defense witness not subject to the protective order. As a practical matter, the Government should know who the Defense will be eliciting the information from on cross examination. Further, identification of such witnesses is unnecessary and not required by MRE 505(h)(3) or the Court's Protective Order.
- v) **December Litigation re: 505(h) and (i):** The Defense is not sure what litigation the Government is envisioning at p. 5 of its case calendar. The case calendar contemplates (or should contemplate) resolving all 505 issues during the Article 39(a) sessions – not waiting until December to litigate these issues. If the parties waited until December to litigate these issues, the Government requests an additional 60 days to coordinate a response, which brings the calendar to 14 February 2013 (the middle of trial). As such, the Defense recommends resolving all 505(h) and (i) issues as they arise and not in December.

## CONCLUSION

7. The Defense respectfully requests that the Court amend the case calendar to reflect the issues noted by the Defense above.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', with a stylized flourish at the end.

DAVID E. COOMBS  
Civilian Defense Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**Prosecution Request  
for Leave until 14 September 2012  
to Provide Notice and Disclosure  
of Certain Documents**

**25 July 2012**

1. The United States requests leave of the Court until 14 September 2012 for the following: (1) to disclose files not subject to the Court's 22 June 2012 order, if any, to the defense or to the Court for *in camera* review IAW RCM 701(g)(2) or MRE 505(g)(2), but which may contain discoverable material, or, (2) if necessary, to notify the Court with a status of whether the United States anticipates the custodian of classified evidence will claim a privilege IAW MRE 505(c) for the classified information under that entity's control and to file notice IAW MRE 505(i)(2).
2. The United States is in the process of completing its review of information that is not under the possession, custody, or control of military authorities and has not been specifically requested by the defense<sup>1</sup> that is owned by the Central Intelligence Agency (CIA), the Department of Homeland Security (DHS), and Office of the Director of National Intelligence (ODNI).<sup>2</sup> The United States is reviewing the information in accordance with their ethical obligation to search for potential *Brady* material and/or their legal obligations under *Williams* in accordance with the Court's 22 June 2012 Order.
3. Although the Court has not set a disclosure date for all *Brady* material, the United States has proposed a disclosure date on its case calendar of 3 August 2012 for all remaining *Brady* material. See Appellate Exhibit CXCIV. The United States is thus requesting leave to complete its review of the CIA and DHS files, and obtain the approval to disclose to the defense any discoverable information in the ODNI, CIA, and DHS files. The United States will not be able to complete its review and obtain the appropriate approvals, if any, by 3 August 2012, because the majority of the information is classified above the "secret" level, contains specialized control measures, or requires interagency coordination.
4. The United States recently completed its review of information at ODNI, and anticipates completing its review of information owned by the DHS and CIA by 27 July 2012. Additionally, while the United States is reviewing documents at the CIA, it will concurrently review for material that is responsive to the defense's recent discovery request dated 19 August 2012.
5. This request will not necessitate a delay in the proceedings as the continued effort to obtain and release this information will occur concurrently with the scheduled pretrial motions process.

<sup>1</sup> On 19 July 2012 and based on their review of the CIA Task Force report, the defense submitted a handwritten motion classified above the "secret" level or containing specialized control measures which requests information that could be contained in the remaining information available for the prosecution's review at the CIA.

<sup>2</sup> This information does not include the Office of the National Counterintelligence Executive (NCIX) damage assessment, which was the subject of the Court's 22 June 2012 Order.

APPELLATE EXHIBIT 326  
PAGE REFERENCE  
PAGE \_\_\_ OF \_\_\_ PAGES



Additionally, the United States does not anticipate this request affecting the approval process or disclosure date of the follow-on report to the CIA's WikiLeaks Task Force Report, which the prosecution gave notice to the Court on 12 July 2012. *See* Appellate Exhibit CCVIII. There will, therefore, be no prejudice to the defense.

A handwritten signature in black ink, consisting of a large, stylized capital 'A' followed by a cursive 's' and a horizontal line.

ASHDEN FEIN  
MAJ, JA  
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 25 July 2012.

A handwritten signature in black ink, consisting of a large, stylized capital 'A' followed by a cursive 's' and a horizontal line.

ASHDEN FEIN  
MAJ, JA  
Trial Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

**MANNING, Bradley E., PFC**

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

)  
)  
) **DEFENSE RESPONSE TO**  
) **PROSECUTION REQUEST FOR**  
) **LEAVE TO UNTIL 14**  
) **SEPTEMBER 2012 TO PROVIDE**  
) **NOTICE AND DISCLOSURE OF**  
) **CERTAIN DOCUMENTS**

) DATED: 26 July 2012  
)

RELIEF SOUGHT

1. PFC Bradley Manning, by and through the undersigned Defense counsel, opposes the Government's request for leave of Court until 14 September 2012 for the following: (1) to disclose files not subject to the Court's 22 June 2012 order, if any, to the defense or to the Court for *in camera* review IAW RCM 701(g)(2) or MRE 505(g)(2), but which may contain discoverable material, or, (2) if necessary, to notify the Court with a status of whether the United States anticipates the custodian of classified evidence will claim a privilege IAW MRE 505(c) for the classified information under that entity's control and to file notice IAW MRE 505(i)(2). The Defense requests that the Court order the Government to respond by 3 August 2012.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Government has the burden of persuasion. RCM 905(c)(2)(A). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

3. On 22 June 2012, the Court ordered the Government to provide discovery under a timeline that would result in all discovery issues being addressed by 3 August 2012. The Government incorporated this 3 August 2012 timeline into its proposed case calendar.

4. The Government admits that it has already completed its review of Office of the Director of National Intelligence (ODNI) information. It also anticipates completing its review of information owned by the Department of Homeland Security (DHS) and Central Intelligence Agency (CIA) by 27 July 2012.

APPELLATE EXHIBIT 227  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

## ARGUMENT

5. The Government is requesting an additional 43 days to produce certain *Brady* discovery in this case. Under the Court's original timeline – which the Government voluntarily adopted – the Government had 43 days to produce this *Brady* discovery or claim a privilege. An additional 43 days is not an “extension.” It is double the amount of time that the Court deemed appropriate for the Government to comply with its *Brady* obligations.

6. It must not be forgotten that the Government has had well over two years to conduct discovery in this case. There is no reason why the Government should not already have reviewed the relevant files and be prepared to proceed accordingly. The Government seems to think that by underlining the word “not” in its motion, this should somehow make a difference to the Court's determination (“The United States is in the process of completing its review of information that is not under the possession, custody, or control of military authorities and has not been specifically requested by the defense that is owned by the Central Intelligence Agency (CIA), the Department of Homeland Security (DHS), and Office of the Director of National Intelligence (ODNI).”) (emphasis in original). Whether such information was specifically requested is irrelevant to the question of whether the Government should be entitled to an extension. This is *Brady* information that the Government has an obligation to disclose “as soon as practicable” in accordance with R.C.M. 701(a)(6).

7. The Government admits that, as of 27 July 2012, it will have reviewed all the files that are the subject of its motions. However, it states that “because the majority of the information is classified above the ‘secret’ level, contains specialized control measures, or requires interagency coordination” this Court should provide the Government with an extension. The Government fails to explain why *this particular classified discovery* cannot be produced in a timely manner. The vast majority of discovery in this case is classified, requires specialized handling procedures and interagency coordination. This information is no different than the information that will be produced to the Court on 3 August 2012 – already several months after the Defense's original filing of its Motion to Compel Discovery #2.

8. The Government fails to explain why it needs an additional 43 days to produce this discovery as per the Court's order. The Government's rote recitation that “this is complicated” should not continue to provide it with a basis to kick its discovery obligations down the road. Moreover, this Court's case calendar should not be at the continual mercy of “the equity holders” who should have already been consulted long ago about the *Brady* discovery in this case. The Government has known that it needed to provide *Brady* discovery since charges were initially preferred on 5 July 2010. How can it be that after all this time, the Government has not properly coordinated with key agencies in this case (in particular, the CIA and ODNI)? If an extra 43 days is the magic number, why did the Government not coordinate with these agencies 43 days earlier?<sup>1</sup>

---

<sup>1</sup> Note that the Government's *Brady* obligations existed irrespective of the Defense's motions to compel discovery. In other words, it was not the Court's 22 June 2012 ruling that precipitated the necessity for the Government to review files from CIA, ODNI and DHS. As such, the Government should have already been coordinating with these agencies long ago.

9. The Court's order contemplates all discovery being either in the Defense's hands or in the Court's hands for *in camera* review by 3 August 2012 (or that the procedures for claiming a privilege will be set in motion by that date). That way, discovery disputes will largely be resolved by early September, prior to the Defense's filing of its speedy trial motion. The Government's current motion asks for until 14 September 2012 to notify the Court of whether it anticipates that a custodian of classified information will claim a privilege. If so, time will then need to be built-into the calendar to brief and argue the privilege issues, likely bringing this discovery issue into the November time period.

10. In ordering the Government to produce a due diligence statement, this Court was cognizant that the discovery issues would impact the Defense's presentation, and Court's assessment of, the speedy trial motion. The court noted, "This Court must rule upon the motions to compel discovery that have been filed in this case and a speedy trial motion to be filed by the Defense. One document containing the information in paragraph (2) above will assist the Court in addressing discovery and speedy trial issues arising during the trial." Appellate Exhibit CLXXVII. The Court also noted that "the case calendar will continue into July and August with scheduled motions that are not impacted by receipt of defense discovery." *Id.* Clearly, the Court was contemplating having the discovery issues largely resolved in August, so that the Defense could file its speedy trial motion in early September.

11. The Government's request for an additional 43 days – pushing back the timeline to 14 September 2012 (and possibly much later) – will impact the Defense's speedy trial motion. The Government's diligence in seeking out and providing discovery is part and parcel of any speedy trial motion. Where discovery issues are still up in the air, the Defense is not able to properly present its case arguing a violation of the accused's speedy trial rights. The Defense should not be required to present a less-than-fulsome speedy trial motion while the Government gets a 43-day extension to complete the *Brady* obligations it should have completed long ago. This Court has said that "both parties will have an opportunity to litigate the due diligence of the Government in providing discovery during the speedy trial motion." *Id.* If the Government has not yet provided the discovery that is the subject of the speedy trial motion, how can the Defense have an adequate opportunity to litigate the due diligence issue? This is particularly so given the Court's ruling that the Government should be granted a nearly two month extension for the Department of State discovery. See Appellate Exhibit CCXXII. If significant discovery issues are still unresolved (State Department discovery, CIA discovery, ODNI discovery and DHS discovery – plus any ancillary issues arising from this discovery), the Defense is seriously hampered in its ability to address, in a complete and compelling manner, the speedy trial issues in this case.

12. The Defense submits that the Government has not provided any legitimate justification for an extension of double the original timeline. Moreover, any such extension would impact the Defense's speedy trial motion. As such, the Defense requests that this Court deny the Government's motion for an extension of time.

## CONCLUSION

13. For the above reasons, the Defense requests that the Court deny the Government's request for an extension of time, and order the Government to respond by 3 August 2012.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Coombs', with a stylized flourish at the end.

DAVID E. COOMBS  
Civilian Defense Counsel

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Supplement to Prosecution Request  
for Leave until 14 September 2012  
to Provide Notice and Disclosure  
of Certain Documents

31 July 2012

1. On 25 July 2012, the prosecution requested leave of the Court until 14 September 2012 for the following: (1) to disclose records owned by the Central Intelligence Agency (CIA), the Department of Homeland Security (DHS), and Office of the Director of National Intelligence (ODNI) not subject to the Court's 22 June 2012 order, if any, to the defense or to the Court for *in camera* review IAW RCM 701(g)(2) or MRE 505(g)(2), but which may contain discoverable material, or, (2) if necessary, to notify the Court with a status of whether the prosecution anticipates the custodian of such records will claim a privilege IAW MRE 505(c) for the classified information under that entity's control and to file notice IAW MRE 505(i)(2). On 26 July 2012, the defense opposed.
2. On 26 July 2012, the Court ordered the prosecution to "file a supplemental pleading stating with particularity the review and approval procedures required prior to disclosure of information above the 'secret' level and how that differs from the review and approval procedures required prior to disclosure of information at or below the 'secret' level."

### SPECIFIC APPROVAL PROCEDURES

3. Much of the information underlying the prosecution's request includes information above the "SECRET" level and sensitive compartmented information (SCI). See Army Regulation (AR) 380-5, para. 2-10 (TOP SECRET classification is "applied to information in which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security"<sup>1</sup>); see also Director of Central Intelligence Directive 6/1 (SCI is defined as "[c]lassified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled exclusively within formal access control systems established by the Director of Central Intelligence"). Some of the material also includes Foreign Intelligence Surveillance Act (FISA) information. The most important difference between the approval process for SCI or "TOP SECRET" information and information below the "SECRET" level is that Original Classification Authority (OCA) for "SECRET" information is generally delegated to a much lower level, requiring less coordination with senior officials within and among organizations. Disclosure of classified information to the defense must be approved by the relevant OCA.

<sup>1</sup> SECRET classification is "applied to information in which the unauthorized disclosure could reasonably be expected to cause serious damage to the national security." AR 380-5.

4. **CIA.** In order to obtain approval to disclose potentially discoverable information at the CIA, each component with equities in the information (e.g. National Clandestine Service or Directorate of Intelligence) must be consulted and coordinated with prior to disclosure. This ensures that intelligence sources and methods are protected and is true whether the information is classified "SECRET" or "TOP SECRET." The CIA generally "owns" most of the intelligence incorporated into its documents and information, but because much of that information is SCI, the approval process takes additional time. Additionally, the process is delayed because of the sensitivity of sources and methods and the special handling procedures required. SCI must be reviewed in a Sensitive Compartmented Information Facility and cannot be shared over the SIPRNET with the prosecution, requiring travel that may delay the process based on the availability of essential personnel, such as the assigned litigation attorney from the organization.

5. **DHS and ODNI.** DHS and ODNI are not collectors of information. ODNI operates to effectively integrate foreign, military and domestic intelligence—they are a customer of information. The same is true for DHS. DHS and ODNI rely on the intelligence collected by the CIA and National Security Agency, among others, and incorporate the intelligence collected by those organizations into their own products. Thus, DHS and ODNI records may consist largely of SCI owned by other government organizations, and ODNI and DHS must seek the approval of those other organizations in order to ultimately approve disclosure of their information to the defense. This process differs from information at the "SECRET" level or below because less sensitive information can be shared over the SIPRNET, or the prosecution may disseminate the information on ODNI's behalf to speed up the approval process.

6. **FISA Information.** The Attorney General of the United States must approve in advance the disclosure of any FISA materials. See 50 U.S.C. 1806(b). The prosecution has yet to disclose FISA information in this case and should any FISA information be discoverable, will have to coordinate through the Department of Justice for approval to disclose to the defense.

  
JODEAN MORROW  
CPT, JA

Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel, via electronic mail, on 31 July 2012.

  
JODEAN MORROW  
CPT, JA

Assistant Trial Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

)  
)  
) **DEFENSE RESPONSE TO**  
) **PROSECUTION SUPPLEMENT**  
) **TO REQUEST FOR LEAVE**  
) **UNTIL 14 SEPTEMBER 2012 TO**  
) **PROVIDE NOTICE AND**  
) **DISCLOSURE OF CERTAIN**  
) **DOCUMENTS**

) DATED: 1 AUGUST 2012  
)

RELIEF SOUGHT

1. PFC Bradley Manning, by and through the undersigned Defense counsel, opposes the Government's request for leave of Court until 14 September 2012 for the following: (1) to disclose files not subject to the Court's 22 June 2012 order, if any, to the defense or to the Court for *in camera* review IAW RCM 701(g)(2) or MRE 505(g)(2), but which may contain discoverable material, or, (2) if necessary, to notify the Court with a status of whether the United States anticipates the custodian of classified evidence will claim a privilege IAW MRE 505(c) for the classified information under that entity's control and to file notice IAW MRE 505(i)(2). The Defense requests that the Court order the Government to respond by 3 August 2012. In the alternative, the Defense requests that the Government be required to disclose any material classified "secret" or below by 3 August 2012.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Government has the burden of persuasion. RCM 905(c)(2)(A). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

3. On 22 June 2012, the Court ordered the Government to provide discovery under a timeline that would result in all discovery issues being addressed by 3 August 2012. The Government incorporated this 3 August 2012 timeline into its proposed case calendar.

4. On 31 July 2012, per the Court's order on 26 July 2012, the Government provided the Court with a supplement to its request for leave dated 25 July 2012.



## ARGUMENT

5. While the Government's supplement addresses some differences in the approval process material classified above "secret", it fails to explain why, after over two years of litigation, they have not already taken the necessary steps to obtain the requisite authorities for disclosure. Indeed, the Government has known since this case's infancy that it involved large amounts of classified material. Likewise, the Government should have been aware of its obligations under *Brady*. The Government has had more than enough time to review the relevant files, make *Brady* determinations, coordinate with OCAs, discuss privileges and make necessary disclosures to the Court and the Defense. As such, the Defense requests the Court require the Government to comply with the ordered 3 August disclosure date.

6. On 26 July, the Court ordered the Government to "file a supplemental pleading stating with particularity the review and approval procedures required prior to disclosure of information above the "secret" level and how that differs from the review and approval procedures required prior to disclosure of information at or below the "secret" level." The Government notes that often approval for disclosure of material classified at a "secret" level is delegated below the OCA. However, that Government fails to address whether that is the case with the agencies relevant to the instant request. Moreover, the Government fails to establish how any variance in the disclosure process warrants an extension.

- a. CIA. The Government admits that the same equities have to be consulted regardless of whether a document is classified "secret" or "top secret." This being the case the Government should be able to meet the 3 August deadline.
- b. DHS and ODNI. The Government notes that much of the material from these agencies comes from the CIA. As is already established, the process for CIA disclosure does not vary between "secret" and "top secret." As such, it does not seem that any additional time would be warranted
- c. FISA. The Government does not address any variance of disclosure procedures between classification levels for this type of information.

7. Certainly after two years of litigation and seemingly endless coordination with "equity holders" the Government has developed a working relationship with the various agencies that can foster some expediency.

8. Further, the Government fails to address why it cannot produce those relevant documents that are classified "secret" or below on 3 August 2012. Such documents do not require the additional measures that serve as the basis for the Government request and, as such, should be disclosed to the Defense, pursuant to the Court's 22 June order, on 3 August.

9. The Defense submits that the Government has had adequate time to accomplish the task for which it requests the Court's leave. Moreover, the Government has failed to adequately address the Court's query as to the differences in procedures for gaining permission to disclose documents at varying classification levels. As such, the Government should be required to make

all disclosures on 3 August 2012. Alternatively, the Defense request the Government be required to disclose all material classified as "secret" or below on 3 August 2012.

CONCLUSION

10. For the above reasons, the Defense requests that the Court deny the Government's request for an extension of time, and order the Government to respond by 3 August 2012. In the alternative, the Defense requests that, at a minimum, the Government be required to disclose all material classified as "secret" or below by 3 August 2012.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Joshua J. Tooman', written over a horizontal line.

JOSHUA J. TOOMAN  
Defense Counsel

UNITED STATES OF AMERICA )

v. )

**Manning, Bradley E.**  
**PFC, U.S. Army,**  
**HHC, U.S. Army Garrison,**  
**Joint Base Myer-Henderson Hall**  
**Fort Myer, Virginia 22211**

) **RULING: GOVERNMENT**  
) **REQUEST FOR LEAVE UNTIL 14**  
) **SEPTEMBER 2012 TO PROVIDE**  
) **NOTICE AND DISCLOSURE OF**  
) **CERTAIN DOCUMENTS**  
) **DATED: 1 August 2012**

The Government requests leave of the Court until 14 September 2012 for the following: (1) to disclose files not subject to the Court's 22 June 2012 order but which may contain discoverable material, if any, to the defense or to the Court for *in camera* review IAW RCM 701(g)(2) or MRE 505(g)(2), or, (2) if necessary, to notify the Court with a status of whether the United States anticipates the custodian of classified evidence will claim a privilege IAW MRE 505(c) for the classified information under that entity's control and to file notice IAW MRE 505(i)(2). The reason cited by the Government for the request is that the majority of the information is classified above the "Secret" level requiring additional time to obtain review and approval required prior to disclosure of the information. Defense opposes. On 26 July 2012 the Court ordered the Government to file a supplemental pleading stating with particularity the review and approval procedures required prior to disclosure of information classified above the "Secret" level and how that differs from the review and approval procedures required prior to disclosure of information at or below the "secret" level. Both parties filed supplemental responses. Having considered the filings of the parties, the Court rules as follows:

1. The information at issue in this request is information classified at the "secret" or above "secret" level that is owned by the Central Intelligence Agency (CIA), the Department of Homeland Security (DHS), and the Office of the Director of National Intelligence (ODNI) and possibly information falling within the Foreign Intelligence Surveillance Act (FISA). Further, on 19 July 2012, the Defense submitted a discovery request for additional CIA information. The discovery request was classified above the "secret" level or containing specialized control measures.
2. The Government has advised the Court that it anticipates completing its review of information owned by DHS, and CIA by 27 July 2012, to include information responsive to the Defense 19 July 2012 discovery request. The Government further advised the Court that it will not be able to complete its review and obtain appropriate approvals by 3 August 2012 date set forth by the court calendar because the majority of the information is classified above the "secret" level, contains specialized control measures, or requires interagency coordination.
3. This is a complex case involving hundreds of thousands of classified documents that are potentially discoverable. There are statutory and regulatory requirements as well as interagency coordination processes that the Government must meet in order to disclose discoverable classified information to the Defense. The rules in MRE 505 recognize the special procedures required for disclosure of classified information. Accordingly, the reasons identified by the Government and the time period are reasonable.

APPELLATE EXHIBIT 230  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

**RULING:**

1. Upon receipt of agency approval to disclose discoverable classified information to the Defense, or to the Court IAW RCM 701(g)(2) or MRE 505(g)(2), the Government will immediately disclose that information to the Defense and/or the Court.
2. Except as provided in (1) above, the Government request for Leave until 14 September 2012 is **GRANTED**.

**SO ORDERED** this 1<sup>st</sup> Day of August 2012.



DENISE R. LIND  
COL., JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, [REDACTED]  
Headquarters and Headquarters Company, U.S.  
Army Garrison, Joint Base Myer-Henderson Hall,  
Fort Myer, VA 22211

**DEFENSE REQUEST FOR  
CONTINUANCE**

DATED: 27 July 2012

FACTS

1. PFC Manning was held at Marine Corps Base Quantico from 29 July 2010 to 20 April 2011. During this time, PFC Manning was held in MAX custody and under Prevention of Injury watch.
2. In the fall of 2010, the Defense raised the issue of unlawful pretrial punishment with the Government. On 8 December 2010, the Defense made a discovery request for all documentation from Quantico pertaining to PFC Manning.
3. The Government provided extensive documentation related to PFC Manning's confinement at Quantico in October of 2011. The Defense believed that this was the full extent of the information the Government had from Quantico.
4. The Article 13 motion has been on the case calendar since this case was referred. The deadline for the Defense to file the Article 13 motion was today, 27 August 2012. The Defense had already advised the Government that this was a very lengthy and involved motion, totaling over 100 pages. In fact, the case calendar had accommodated the Government's request for an additional week to respond to the motion.
5. On 26 August, the Defense informed the Court and the Government that it would be sending the attachments for the Article 13 motion by Fed-Ex. The attachments exceed 500 pages. The Government did not indicate to the Defense not to mail the attachments.
6. On the evening of 26 August (after the Defense's attachments had already been sent), MAJ Fein sent Mr. Coombs the following email at 19:50:

In preparation for the upcoming Article 13 motion, the prosecution began reviewing emails yesterday from members of the Quantico brig staff and the chain of command. The prosecution found some emails that are obviously material to the preparation of the defense for Article 13 purposes. In an effort to get these emails to you as soon as possible, we intend to produce them tomorrow and send

1  
JUL 27 2012 19:50  
TACD REFERENCED  
PAGE 1 OF 231 PAGES

them to you via email so that you have a copy immediately. We will also produce them according to our normal process. We estimate there are approximately 60 emails.

See Attachment A. An hour and a half later, at 21:15, MAJ Fein sent the Defense the referenced emails. There were a total of 84 (not 60) emails. See Attachment B.

7. MAJ Fein indicated that the Government received these emails from Quantico approximately 6 months ago. However, the Government did not begin reviewing the emails until two days ago, 25 July 2012.

#### RELIEF SOUGHT

8. In light of the Government's late disclosures and its failure to provide timely discovery, the Defense requests a continuance of the proceedings in order to review and incorporate information from the 84 emails into its Article 13 submissions; to interview (and re-interview) witnesses based on information contained therein; and to file a new witness list and motion to compel witnesses, if necessary.

9. The Defense requests the following changes to the case calendar:

- a) Initial Article 13 Motion – No change;
- b) Defense Second Request for Article 13 Witnesses: 15 August 2012;
- c) Government Objection to Defense Request for Article 13 Witnesses (if any): 22 August 2012;
- d) Defense Supplemental Article 13 Motion: 24 August 2012;
- e) Defense Motion to Compel Article 13 Witnesses (if any): 24 August 2012;
- f) Article 39(a) Session for Article 13 Witnesses and other issues: 28 – 30 August 2012;
- g) Government Response to Defense Article 13 and Supplemental Article 13 Motion: 7 September 2012;
- h) Defense Reply to Government Response to Article 13 Motion: 14 September 2012;
- i) Article 39(a) to litigate the Article 13 Motion: 1 – 5 October 2012.

10. Additionally, the Defense requests that the Article 39(a) sessions and filing deadlines currently scheduled be continued for two weeks. Specifically, the Defense requests that all Speedy Trial filing deadlines be continued for two weeks.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

**ATTACHMENT A**

## David Coombs

---

**From:** Fein, Ashden MAJ USARMY MDW (US) <ashden.fein.mil@mail.mil>  
**Sent:** Thursday, July 26, 2012 7:49 PM  
**To:** David Coombs  
**Cc:** 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, Jeffrey H CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR \MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US)  
**Subject:** Article 13 Emails

David,

In preparation for the upcoming Article 13 motion, the prosecution began reviewing emails yesterday from members of the Quantico brig staff and the chain of command. The prosecution found some emails that are obviously material to the preparation of the defense for Article 13 purposes. In an effort to get these emails to you as soon as possible, we intend to produce them tomorrow and send them to you via email so that you have a copy immediately. We will also produce them according to our normal process. We estimate there are approximately 60 emails.

V/r  
Ashden



**ATTACHMENT B**

## David Coombs

---

**From:** Fein, Ashden MAJ USARMY MDW (US) <ashden.fein.mil@mail.mil>  
**Sent:** Friday, July 27, 2012 8:22 AM  
**To:** Lind, Denise R COL USARMY (US)  
**Cc:** David Coombs; 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR\MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US)  
**Subject:** RE: Article 13 Emails

Ma'am,

Below is the government response to the below email from the defense:

1. On 8 December 2010, the defense requested "[a]ny and all documents or observation notes by employees of the Quantico confinement facility relating to PFC Bradley Manning." The United States produced all documentation from the Quantico Brig either as we received it or at the end of the accused's pretrial confinement at Quantico. In an effort to preserve all records involving the accused, the prosecution requested Quantico preserve all documentation and their emails. The purpose of this preservation request was to ensure the accused's right to a fair trial by preserving any emails for future litigation concerning the discoverability of the emails and/or for the prosecution to conduct a Giglio and Jencks (RCM 914) check of the emails. On Wednesday, the prosecution started reviewing the emails for potential impeachment evidence or Jencks material, and during that review found 84 emails which we deemed obviously material to the preparation of the defense for Article 13 purposes. Within 24 hours, the United States notified the defense and sent the emails last night.
2. The United States objects to the defense's characterization of the emails showing a conspiracy, rather the emails show the possible extent, if any, of USMC chain of command's involvement, in the accused's pretrial confinement.
3. This motions hearing is not scheduled until the end of August. Over the past few months, the defense has been preparing its over 100 page motion and the government has a reply due on 17 August 2012. Understanding Mr. Coombs will be out of the office from 27 July to 9 August, the United States still sees no reason why the defense will not have adequate time to prepare its Article 13 motion, and especially since this the majority of these emails appear to only bolster the defense's current argument, as proffered in the Article 13 witness list litigation. Additionally, the military defense counsel can assist Mr. Coombs with interviewing other potential witnesses, if the defense chooses to go down that path.

v/r  
MAJ Fein

-----Original Message-----

**From:** David Coombs [mailto:coombs@armycourtmarshialdefense.com]  
**Sent:** Friday, July 27, 2012 12:54 AM  
**To:** Lind, Denise R COL USARMY (US)  
**Cc:** 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR\MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Fein, Ashden MAJ USARMY MDW (US)  
**Subject:** RE: Article 13 Emails  
**Importance:** High

Ma'am,

Please see the email below. MAJ Fein just notified the Defense of the existence of 60 emails that the Government determined were material to the

preparation of the defense for the Article 13 motion which, as you know, is due tomorrow. At 2115, MAJ Fein sent the Defense copies of the emails. The Defense cannot understand why it is getting these emails the night before its motion is due. The Defense had requested any documentation pertaining to PFC Manning's confinement while at Quantico over a year and a half ago, in a discovery request dated 8 December 2010.

After quickly reviewing the emails sent by MAJ Fein, it is clear that we have a problem. The Defense had previous knowledge that there had been an order given by the Security Battalion Commander, Col. Robert Oltman, to keep PFC Manning in maximum custody and under prevention of injury status indefinitely. This order was given on 13 January 2011 and was made in front of the Brig commander and staff. Capt. William Hocter and Capt. Kevin Moore witnessed this order and would be testifying to this fact during the motions hearing. The emails that the Defense has just received reveal a conspiracy at much higher levels.

The email traffic shows that LtGen. George Flynn was directly involved in the custody status of PFC Manning. The Quantico Base Commander, Col. Daniel Choike, and Col. Robert Oltman seem to have been simply executing LtGen. Flynn's directives. The emails show how the entire chain of command from LtGen. Flynn down to the NCO leadership in the Brig was involved in reporting on every issue dealing with PFC Manning in order to support the decision to maintain him in his custody status. The emails also show that the Quantico Staff Judge Advocate, LtCol. Christopher Greer, was aware of the issue and supported the chain of command's efforts. In addition to this, the Defense has learned many more specifics about the nature of PFC Manning's confinement conditions which support his Article 13 claim.

This new information will result in a need for additional witnesses. And, as is no doubt apparent, it will require additional time to brief. As you know, I have already completed what I believed was the Defense's Article 13 motion and have sent the Court and the Government the attachments.

As I previously informed the Court and the Government, I will be out of the office from 27 July through 9 August for family reasons. At this point, I am unclear on how to proceed. I would greatly appreciate guidance from the Court in this respect.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
coombs@armycourt martialdefense.com  
www.armycourt martialdefense.com

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

)  
) **RULING: DEFENSE REQUEST**  
) **FOR CONTINUANCE**

v. )

)  
) **MANNING, Bradley E., PFC**

)  
) **U.S. Army, [REDACTED]**

)  
) **Headquarters and Headquarters Company, U.S.**

)  
) **Army Garrison, Joint Base Myer-Henderson Hall,**  
) **Fort Myer, VA 22211**

) **DATED: 1 August 2012**

On 27 July 2012, the Defense requested the following adjustments to the case calendar based on the Government's 26 July 2012 disclosure of 84 emails germane to the preparation of the Defense Article 13 motion that was due to the Court on 27 July 2012:

- a) Initial Article 13 Motion – No change;
- b) Defense Second Request for Article 13 Witnesses: 15 August 2012;
- c) Government Objection to Defense Request for Article 13 Witnesses (if any): 22 August 2012;
- d) Defense Supplemental Article 13 Motion: 24 August 2012;
- e) Defense Motion to Compel Article 13 Witnesses (if any): 24 August 2012;
- f) Article 39(a) Session for Article 13 Witnesses and other issues: 28 – 30 August 2012;
- g) Government Response to Defense Article 13 and Supplemental Article 13 Motion: 7 September 2012;
- h) Defense Reply to Government Response to Article 13 Motion: 14 September 2012;
- i) Article 39(a) to litigate the Article 13 Motion: 1 – 5 October 2012.

The Defense also requested that the Article 39(a) sessions and filing deadlines currently scheduled be continued for two weeks and that all Speedy Trial filing deadlines be continued for two weeks.

The Court calendar set 27 July 2012 as the filing deadline for the Defense Article 13 motion. The motion was scheduled to be litigated during the 27-31 August 2012 Article 39(a) session. On 26 July 2012, the Government disclosed 84 emails obviously material to the preparation of the Defense Article 13 motion. Mr. Coombs notified the Court prior to 27 July 2012 that he would be out of the country from 27 July 2012 – 9 August 2012. Upon receiving the emails from the Government the night before the Article 13 motion was due to the Court, the Defense sent an email to the Court advising that the Defense would need more time to incorporate the information gleaned from the 84 emails into its Article 13 motion and to identify and interview additional witnesses for the Article 13 motion. The Government opposed the Defense email request for a continuance. The series of emails exchanged between the parties and the Court on 27 July 2012 are attached to this order.

The Court held a telephonic RCM 802 conference with the parties on 27 July 2012 to address the Defense request for adjustments to the trial schedule. CPT Overgaard represented the Government. Mr. Coombs represented the Defense. The parties and the Court arrived at the following mutually agreeable case calendar:

1. Article 13 motion, response, reply - no change.
2. Defense 2nd request for Article 13 witnesses:
  - 15 August 2012- defense request
  - 22 August 2012- government objections
  - 24 August 2012- defense motion to compel
  - 28-30 August 2012 - Article 39(a) session (reduced from 5 - 3 days due to Article 13 litigation continuance)
3. Defense supplemental Article 13 motion:
  - 24 August 2012- defense filing
  - 7 September 2012 - government response
  - 14 September 2012 - defense reply
  - 1-5 October 2012 - Article 39(a) to litigate Article 13
4. The Article 39(a) sessions and filing deadlines currently scheduled to begin 15 October and 27 November are each continued for 2 weeks. The Article 39(a) schedule set to begin 7-11 January 2013 is continued 1 week. The final motions session scheduled to begin on 30 January 2012 will remain as scheduled. Thus, the following dates are scheduled:

Article 39(a):

28-30 August 2012  
1-5 October 2012  
29 October - 2 November 2012  
10-14 December 2012  
14-18 January 2013  
28 January -29 January 2013

Trial: 30-31 January 2013 (voir dire)  
4-22 February 2013 (trial)

The Court ordered the Government to produce a draft case calendar reflecting the above changes. After the telephonic RCM 802 conference, the Government raised concerns regarding suspense dates for MRE 505(h) notice, witness lists, reciprocal discovery, accused's plea and forum selection, notice of defense of lack of mental responsibility, and disclosure of RCM 914 material. The Government also advised the Court that the Presidential Inauguration period scheduled 15-24 January 2012 will cause logistics and administrative issues if proceedings for this case are scheduled during that period.

**RULING:** The Defense Motion for a Continuance is **GRANTED** as set forth above. The Court calendar is adjusted as agreed to by the Parties during the telephonic RCM 802 conference. During the 28-30 August 2012 Article 39(a) session, the parties and the Court will review the Case calendar once again and make any necessary adjustments to suspense dates, Article 39(a) dates, and trial dates.

**SO ORDERED** this 1<sup>st</sup> Day of August 2012.

A handwritten signature in black ink, appearing to read 'DRL' with a stylized flourish at the end.

DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

**From:** [coombs@armycourt martialdefense.com](mailto:coombs@armycourt martialdefense.com)  
**To:** [Lind, Denise R COL USARMY \(US\)](mailto:Lind, Denise R COL USARMY (US) <denise.r.lind.mil@mail.mil>); [Overgaard, Angel M CPT USARMY \(US\)](mailto:Overgaard, Angel M CPT USARMY (US) <angel.m.overgaard.mil@mail.mil>)  
**Cc:** "Hurley, Thomas F MAJ OSD OMC Defense"; [Tooman, Joshua J CPT USARMY \(US\)](mailto:Tooman, Joshua J CPT USARMY (US) <joshua.j.tooman.mil@mail.mil>); "Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA"; [Whyte, J Hunter CPT USARMY \(US\)](mailto:Whyte, J Hunter CPT USARMY (US) <jeffrey.h.whyte.mil@mail.mil>); [VonElten, Alexander S. CPT USA JFHQ-NCR/MDW SJA](mailto:VonElten, Alexander S. CPT USA JFHQ-NCR/MDW SJA); [Ford, Arthur D Jr CW2 USARMY \(US\)](mailto:Ford, Arthur D Jr CW2 USARMY (US) <arthur.d.ford.mil@mail.mil>); [Fein, Ashden MAJ USARMY MDW \(US\)](mailto:Fein, Ashden MAJ USARMY MDW (US) <ashden.fein.mil@mail.mil>); [Parra, Jairo A \(JP\) CW2 USARMY USAMDW \(US\)](mailto:Parra, Jairo A (JP) CW2 USARMY USAMDW (US) <jairo.a.parra.mil@mail.mil>)  
**Subject:** RE: Court Calendar and Article 13 motion  
**Date:** Friday, July 27, 2012 4:09:23 PM

---

Ma'am,

The Defense does not object to the dates listed by the Court, and will file its request for a continuance along with it Article 13 motion later today.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourt martialdefense.com](mailto:coombs@armycourt martialdefense.com)  
[www.armycourt martialdefense.com](http://www.armycourt martialdefense.com) <<http://www.armycourt martialdefense.com/>>

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

----- Original Message -----

**Subject:** Court Calendar and Article 13 motion  
**From:** "Lind, Denise R COL USARMY (US)" <[denise.r.lind.mil@mail.mil](mailto:denise.r.lind.mil@mail.mil)>  
**Date:** Fri, July 27, 2012 3:53 pm  
**To:** "Overgaard, Angel M CPT USARMY (US)" <[angel.m.overgaard.mil@mail.mil](mailto:angel.m.overgaard.mil@mail.mil)>, David Coombs <[coombs@armycourt martialdefense.com](mailto:coombs@armycourt martialdefense.com)>  
**Cc:** "Hurley, Thomas F MAJ OSD OMC Defense" <[thomas.hurley@osd.mil](mailto:thomas.hurley@osd.mil)>, "Tooman, Joshua J CPT USARMY (US)" <[joshua.j.tooman.mil@mail.mil](mailto:joshua.j.tooman.mil@mail.mil)>, "Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA" <[JoDean.Morrow@jfhqncr.northcom.mil](mailto:JoDean.Morrow@jfhqncr.northcom.mil)>, "Whyte, J Hunter CPT USARMY (US)" <[jeffrey.h.whyte.mil@mail.mil](mailto:jeffrey.h.whyte.mil@mail.mil)>, "von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA" <[Alexander.VonElten@jfhqncr.northcom.mil](mailto:Alexander.VonElten@jfhqncr.northcom.mil)>, "Ford, Arthur D Jr CW2 USARMY (US)" <[arthur.d.ford.mil@mail.mil](mailto:arthur.d.ford.mil@mail.mil)>, "Fein, Ashden MAJ USARMY MDW (US)" <[ashden.fein.mil@mail.mil](mailto:ashden.fein.mil@mail.mil)>, "Parra, Jairo A (JP) CW2 USARMY USAMDW (US)" <[jairo.a.parra.mil@mail.mil](mailto:jairo.a.parra.mil@mail.mil)>

Counsel,

Assuming I receive a motion from the defense, the parties and the Court arrived at the below mutually agreeable case calendar during the telephonic RCM 802 conference held today between the Court, CPT Overgaard, and Mr. Coombs:

1. Article 13 motion, response, reply - no change.

2. Defense 2nd request for Article 13 witnesses:  
15 August - defense request  
22 August - government objections  
24 August - defense motion to compel  
28-30 August - Article 39(a) session (reduced from 5 - 3 days due to Article 13 litigation continuance)

3. Defense supplemental Article 13 motion:  
24 August - defense filing  
7 September - government response  
14 September - defense reply  
1-5 October 2012 - Article 39(a) to litigate Article 13

4. The Article 39(a) sessions and filing deadlines currently scheduled to begin 15 October and 27 November are each continued for 2 weeks. The Article 39(a) schedule set to begin 7-11 January is moved 1 week. The final motions session scheduled to begin on 30 January will remain as scheduled. Thus, the following dates are scheduled:

Article 39(a):

28-30 August 12  
1-5 October 12  
29 October - 2 November 12  
10-14 December 12  
14-18 January 12  
28 January -29 January 2013

Trial: 30-31 January 2013 (voir dire)  
4-22 February 2013 (trial)

D

DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

-----Original Message-----

From: Overgaard, Angel M CPT USARMY (US)

Sent: Friday, July 27, 2012 1:40 PM

To: Lind, Denise R COL USARMY (US); David Coombs

Cc: Hurley, Thomas F MAJ OSD OMC Defense; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Fein, Ashden MAJ USARMY MDW (US); Parra, Jairo A (JP) CW2 USARMY USAMDW (US)

Subject: RE: Article 13 Emails - Government - confirm receipt (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

Ma'am:

Receipt confirmed. We are working to set it up for all to call in at 1515.  
Otherwise, we can just conference in the Court and Mr. Coombs. Thank you.

VR



ANGEL OVERGAARD  
CPT, JA  
Trial Counsel, MDW

-----Original Message-----

From: Lind, Denise R COL USARMY (US)  
Sent: Friday, July 27, 2012 1:35 PM  
To: David Coombs  
Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Fein, Ashden MAJ USARMY MDW (US)  
Subject: RE: Article 13 Emails - Government - confirm receipt

Counsel,

I added CPT Morrow's old email address. Government - confirm receipt and schedule the RCM 802 conference on or after 1515.

D

DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

-----Original Message-----

From: David Coombs [<mailto:coombs@armycourt martialdefense.com>]  
Sent: Friday, July 27, 2012 1:21 PM  
To: Lind, Denise R COL USARMY (US)  
Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Fein, Ashden MAJ USARMY MDW (US)  
Subject: RE: Article 13 Emails

Ma'am,

I am available any time after 1500.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourt martialdefense.com](mailto:coombs@armycourt martialdefense.com)  
[www.armycourt martialdefense.com](http://www.armycourt martialdefense.com)

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the

person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

-----Original Message-----

From: Lind, Denise R COL USARMY (US) [mailto:denise.r.lind.mil@mail.mil]

Sent: Friday, July 27, 2012 1:13 PM

To: David Coombs

Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Fein, Ashden MAJ USARMY MDW (US)

Subject: RE: Article 13 Emails

Counsel,

1. Please confer and schedule a telephonic 802 with me this afternoon. My number is 703-693-0629.
2. Defense - this is a request for a continuance. After the telephonic 802, put the request for continuance in a motion or the schedule remains as is.

D

DENISE R. LIND

COL, JA

Chief Judge, 1st Judicial Circuit

-----Original Message-----

From: David Coombs [mailto:coombs@armycourt martialdefense.com]

Sent: Friday, July 27, 2012 1:10 PM

To: Lind, Denise R COL USARMY (US)

Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Fein, Ashden MAJ USARMY MDW (US)

Subject: RE: Article 13 Emails

Ma'am,

The Defense does have an objection to the proposed schedule. I alerted the Court to the fact that I would be out of the office until 9 August. A deadline of 15 August does not give me sufficient time to prepare a supplementary filing. The Government has just informed the Defense that it has had these emails in its possession for six months, but only recently chose to look at them. Allowing the Defense essentially 6 days (9 August to 15 August) to process all this information is not enough time. Further, three days is not a sufficient amount time to Reply to the Government's Response (to what will be likely 150 pages of Defense filings). The Court should recall that the Government routinely requests weeks, if not months, to respond to any new issues raised by the Defense.

Perhaps of most concern to me, however, are the witness issues. The Defense will likely be moving to compel some very high-profile witnesses (including

a three star General). I'm not sure how the Court could rule on this issue on 27 August, and have these witnesses at the hearing on 29 August. Further, there may be issues with cooperation from the requested witnesses until they are ordered to be produced. As such, the Defense would need additional time to interview these witnesses.

It seems that continuing with the original motions schedule punishes the Defense for the Government's misconduct in holding onto Brady/Giglio material for half a year. It also rewards the Government for bad behavior (e.g. critical witnesses might not be available for the hearing; the Defense needs to re-interview its existing witnesses).

The only way that the Defense can see proceeding under the original motions schedule (and this would still require the Defense working on only this issue virtually non-stop) is for the Government to be precluded from contesting any new witnesses proposed by the Defense. That way, witness issues are resolved as of now and the Defense can proceed accordingly.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
coombs@armycourt martialdefense.com  
www.armycourt martialdefense.com

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

-----Original Message-----

From: Lind, Denise R COL USARMY (US) [<mailto:denise.r.lind.mil@mail.mil>]  
Sent: Friday, July 27, 2012 12:39 PM  
To: David Coombs  
Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Fein, Ashden MAJ USARMY MDW (US)  
Subject: RE: Article 13 Emails

Counsel,

Is there any good cause objection to the following schedule.

27 July - Defense Article 13 Motion  
15 August - Defense Supplemental Article 13 motion and list of additional witnesses  
21 August - Government response to Article 13 motion and additional defense witnesses  
24 August - Defense reply and motion to compel (if necessary)  
27 August - Litigation on motion to compel witnesses

29-31 August - Litigation of Article 13 motion

D

DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

-----Original Message-----

From: David Coombs [<mailto:coombs@armycourtartialdefense.com>]  
Sent: Friday, July 27, 2012 12:26 PM  
To: Lind, Denise R COL USARMY (US)  
Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Fein, Ashden MAJ USARMY MDW (US)  
Subject: RE: Article 13 Emails

Ma'am,

We believe that the Article 13 motion cannot be litigated as planned. Just looking at the case calendar, the Defense could see the following:

July 27: Defense Initial Article 13 Motion;

August 17: Defense Submission of new Article 13 Witness list;

August 24: Government Objections if any to the Witness list; Defense Supplement to the Article 13 Motion;

August 31: Defense Motion to Compel Witnesses; Government Response to Defense Article 13 Motion and Defense Supplement to the Article 13 Motion;

September 7: Defense Reply to Government Response;

X Date: Article 39(a) to resolve witness issues; and

X Date: Article 39(a) for Article 13 Motion.

The Defense is willing to explore other options, but at this point I am not sure what those other options are.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)  
[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com)

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

-----Original Message-----

From: Lind, Denise R COL USARMY (US) [mailto:denise.r.lind.mil@mail.mil]  
Sent: Friday, July 27, 2012 12:05 PM  
To: David Coombs; Fein, Ashden MAJ USARMY MDW (US)  
Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US)  
Subject: RE: Article 13 Emails

Mr. Coombs,

A request for a continuance is a request for more time. It places no responsibility on the defense for causing delay. I take from the below email that the Defense does not move to continue litigation of the Article 39(a) session after the August Article 39(a) and the Defense will:

1. submit the original Article 13 motion today; 2. request the Court to specify a time frame for the Defense to submit a supplement to the Article 39(a) and to request additional witnesses before the 27-31 August article 39(a);

Am I correct?  
D

DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

-----Original Message-----

From: David Coombs [mailto:coombs@armycourtmartrialdefense.com]  
Sent: Friday, July 27, 2012 11:55 AM  
To: Lind, Denise R COL USARMY (US); Fein, Ashden MAJ USARMY MDW (US)  
Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US)  
Subject: RE: Article 13 Emails

Ma'am,

The Defense is not asking for a continuance -- as a continuance implies that somehow the Defense is responsible for these latest events. The Defense has completed a 110 page Article 13 motion and has already Fed-Ex'd attachments to the Court and the Government. The Government allowed the Defense to send its attachments knowing that they were holding on to critical emails that the Defense had no clue even existed.

The Government's untimely disclosures of 84 emails are what has thrown the

Article 13 motion off track. We will have additional witness issues and a need to supplement our Article 13 motion based upon these disclosures.

The Defense is requesting guidance on how the Court would like to address this issue.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
coombs@armycourt martialdefense.com  
www.armycourt martialdefense.com

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

-----Original Message-----

From: Lind, Denise R COL USARMY (US) [<mailto:denise.r.lind.mil@mail.mil>]  
Sent: Friday, July 27, 2012 11:37 AM  
To: David Coombs; Fein, Ashden MAJ USARMY MDW (US)  
Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US)  
Subject: RE: Article 13 Emails

Mr. Coombs,

It appears you are asking the Court for a continuance. Please put the request in a motion and submit it to the Court.

D

DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

-----Original Message-----

From: David Coombs [<mailto:coombs@armycourt martialdefense.com>]  
Sent: Friday, July 27, 2012 8:47 AM  
To: Fein, Ashden MAJ USARMY MDW (US); Lind, Denise R COL USARMY (US)  
Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US)  
Subject: RE: Article 13 Emails

Ma'am,

I have attached one email sent to us late last night by the Government. This email is from the Quantico Base Commander, Col. Daniel Choike, to the Security Battalion Commander, Col. Robert Oltman. Whether this email indicates a conspiracy or just "context" really does not matter at this point (that will be the subject of argument). What matters is that 84 emails were dumped on the Defense the night before the Article 13 motion was due, after I had already sent the Defense attachments and just prior to leaving the country for family reasons.

The Government avoids addressing the two issues that I raised. First, I need additional time to incorporate these emails into my motion. The Government seems to suggest that the emails simply support the arguments that I was in the process of already making, (i.e. I was on the right track). However, these emails do much more than simply support our argument. The emails change the basis of the Defense's argument. When does the Government propose that the Defense incorporate these emails into our motion? Based upon the Government's email it would seem that it would have us do this today.

Second, due to the nature of these emails, the Defense believes that additional witnesses will be needed for the motion. The question is not necessarily just interviewing potential witnesses, but likely litigating with the Government over whether the witnesses will be produced.

How the Government could have waited so long to look at these emails which should have been produced as part of its discovery obligations is beyond me. The fact that the Government is now trying to hold the Defense to a time line of today when the need for a delay is due to their lack of diligence is unbelievable. The Defense has repeated since referral its concern that information would be dumped on us on the eve of trial. This is an perfect example of the Defense's concerns coming to fruition.

v/r

David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282  
coombs@armycourt martialdefense.com

www.armycourt martialdefense.com <<http://www.armycourt martialdefense.com/>>;

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

From: Fein, Ashden MAJ USARMY MDW (US) [<mailto:ashden.fein.mil@mail.mil>]  
Sent: Friday, July 27, 2012 8:22 AM  
To: Lind, Denise R COL USARMY (US)  
Cc: David Coombs; 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US)  
Subject: RE: Article 13 Emails

Ma'am,

Below is the government response to the below email from the defense:

1. On 8 December 2010, the defense requested "[a]ny and all documents or observation notes by employees of the Quantico confinement facility relating to PFC Bradley Manning." The United States produced all documentation from the Quantico Brig either as we received it or at the end of the accused's pretrial confinement at Quantico. In an effort to preserve all records involving the accused, the prosecution requested Quantico preserve all documentation and their emails. The purpose of this preservation request was to ensure the accused's right to a fair trial by preserving any emails for future litigation concerning the discoverability of the emails and/or for the prosecution to conduct a Giglio and Jencks (RCM 914) check of the emails. On Wednesday, the prosecution started reviewing the emails for potential impeachment evidence or Jencks material, and during that review found 84 emails which we deemed obviously material to the preparation of the defense for Article 13 purposes. Within 24 hours, the United States notified the defense and sent the emails last night.

2. The United States objects to the defense's characterization of the emails showing a conspiracy, rather the emails show the possible extent, if any, of USMC chain of command's involvement, in the accused's pretrial confinement.



3. This motions hearing is not scheduled until the end of August. Over the past few months, the defense has been preparing its over 100 page motion and the government has a reply due on 17 August 2012. Understanding Mr. Coombs will be out of the office from 27 July to 9 August, the United States still sees no reason why the defense will not have adequate time to prepare its Article 13 motion, and especially since this the majority of these emails appear to only bolster the defense's current argument, as proffered in the Article 13 witness list litigation. Additionally, the military defense counsel can assist Mr. Coombs with interviewing other potential witnesses, if the defense chooses to go down that path.

v/r

MAJ Fein

-----Original Message-----

From: David Coombs [<mailto:coombs@armycourtmarialdefense.com>]

Sent: Friday, July 27, 2012 12:54 AM

To: Lind, Denise R COL USARMY (US)

Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, J Hunter CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Fein, Ashden MAJ USARMY MDW (US)

Subject: RE: Article 13 Emails

Importance: High

Ma'am,

Please see the email below. MAJ Fein just notified the Defense of the existence of 60 emails that the Government determined were material to the preparation of the defense for the Article 13 motion which, as you know, is due tomorrow. At 2115, MAJ Fein sent the Defense copies of the emails. The Defense cannot understand why it is getting these emails the night before its motion is due. The Defense had requested any documentation pertaining to PFC Manning's confinement while at Quantico over a year and a half ago, in a discovery request dated 8 December 2010.

After quickly reviewing the emails sent by MAJ Fein, it is clear that we have a problem. The Defense had previous knowledge that there had been an order given by the Security Battalion Commander, Col. Robert Oltman, to keep PFC Manning in maximum custody and under prevention of injury status indefinitely. This order was given on 13 January 2011 and was made in front of the Brig commander and staff. Capt. William Hoxter and Capt. Kevin Moore witnessed this order and would be testifying to this fact during the motions hearing. The emails that the Defense has just received reveal a conspiracy at much higher levels.

The email traffic shows that LtGen. George Flynn was directly involved in the custody status of PFC Manning. The Quantico Base Commander, Col. Daniel Choike, and Col. Robert Oltman seem to have been simply executing LtGen. Flynn's directives. The emails show how the entire chain of command from LtGen. Flynn down to the NCO leadership in the Brig was involved in reporting on every issue dealing with PFC Manning in order to support the decision to maintain him in his custody status. The emails also show that the Quantico Staff Judge Advocate, LtCol. Christopher Greer, was aware of the issue and supported the chain of command's efforts. In addition to this, the Defense has learned many more specifics about the nature of PFC Manning's confinement conditions which support his Article 13 claim.

This new information will result in a need for additional witnesses. And, as is no doubt apparent, it will require additional time to brief. As you know, I have already completed what I believed was the Defense's Article 13 motion and have sent the Court and the Government the attachments.

As I previously informed the Court and the Government, I will be out of the office from 27 July through 9 August for family reasons. At this point, I

am unclear on how to proceed. I would greatly appreciate guidance from the Court in this respect.

v/r

David

David E. Coombs, Esq.

Law Office of David E. Coombs

11 South Angell Street, #317

Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282

coombs@armycourtmarialdefense.com

www.armycourtmarialdefense.com

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

-----Original Message-----

From: Fein, Ashden MAJ USARMY MDW (US) [<mailto:ashden.fein.mil@mail.mil>]

Sent: Thursday, July 26, 2012 7:49 PM

To: David Coombs

Cc: 'Hurley, Thomas F MAJ OSD OMC Defense'; Tooman, Joshua J CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, Jeffrey H CPT USARMY (US); 'von Elten, Alexander S. CPT

USA JFHQ-NCR\MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US)

Subject: Article 13 Emails

David,

In preparation for the upcoming Article 13 motion, the prosecution began reviewing emails yesterday from members of the Quantico brig staff and the chain of command. The prosecution found some emails that are obviously material to the preparation of the defense for Article 13 purposes. In an effort to get these emails to you as soon as possible, we intend to produce them tomorrow and send them to you via email so that you have a copy immediately. We will also produce them according to our normal process. We estimate there are approximately 60 emails.

V/r

Ashden

Classification: UNCLASSIFIED  
Caveats: NONE

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC

U.S. Army, [REDACTED]

Headquarters and Headquarters Company, U.S.

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

)  
)  
)  
)  
)  
)  
)  
**DEFENSE MOTION FOR  
JUDICIAL NOTICE OF  
DISTRIBUTED COMMON  
GROUND SYSTEM-ARMY  
INADEQUACIES**

)  
)  
)  
)  
)  
)  
)  
**DATED: 3 AUGUST 2012**

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, moves this court, pursuant to Military Rule of Evidence (M.R.E.) 201 to take judicial notice of inadequacies with the Distributed Common Ground System-Army (DCGS-A). Specifically, the Defense requests judicial notice that the DCGS-A system was prone to crashes and incapable of functioning when not connected to a network.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Defense has the burden of persuasion. R.C.M. 905(c)(2). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1).

FACTS

3. DCGS-A is "the Army's premier intelligence, surveillance and reconnaissance (ISR) enterprise for the tasking of sensors, analysis and processing of data, exploiting of data and dissemination of intelligence (TPED) across all echelons." *See* Attachment A. Its three core functionalities are serving at the ISR component for Battle Command, providing intelligence analysts a "net enabled capability to exploit information with common analyst tools," and it receives it's data directly from multiple sources. *See* Attachment B. The system provides analysts "access to the multiple databases and near real time direct links from collectors." *Id.*

4. Beginning in 2010, Army and elected officials alike began voicing concerns over the effectiveness of the DCGS-A system.

- a. In a 2 July 2010 memorandum from MG Michael Flynn to the Deputy Commanding General for Support, USFOR-A, MG Flynn asserted, "[i]ntelligence analysts in theater do not have the tools required to fully analyze the tremendous amounts of

APPELLATE EXHIBIT 233

PAGE REFERENCED:

PAGE \_\_\_ OF \_\_\_ PAGES

information currently available in theater.” *See* Attachment C. Specifically, he noted that the systems employed at the time “do not provide the ability to support low-bandwidth or frequently disconnected users with a data sub-set tailored to their area of operations.” *Id.* at 1. MG Flynn goes on to say, “[l]ow bandwidth or frequently disconnected users should be provided a laptop capable of maintaining the data and applications” and “the data set should be updated while the user is connected to the network and should also feed user reports/work back to the central database for wider use.” *Id.* at 2-3.

- b. Members of Congress echoed MG Flynn’s plea, and on 19 July 2010 wrote to the Chairman, the Honorable Norm Dicks and Ranking Member, the Honorable C.W. Young, of the House Appropriations Committee’s Subcommittee on Defense. They wrote, “[a]bove all we ask that funding be provided for a system that can operate remotely while disconnected from the network since DoD has struggled with the issue of connectivity in the remote locations...” *See* Attachment D.
  - c. On 28 July 2010 COL Peter Newell drafted a letter to Chairman Dicks in which he indicated the Army was in the process of implementing a cloud-based tool that would address these concerns. *See* Attachment E.
  - d. Representatives Gabrielle Giffords and Adam Smith responded to COL Newell on 25 August 2010 acknowledging that a cloud-based system, while an upgrade over the then-current system, would still not solve the connectivity issues facing deployed Soldiers. *See* Attachment F.
  - e. On 23 May 2011 Representative Smith sent a letter Chief of Staff, General Martin Dempsey. Representative Smith followed up on the 25 August 2010 letter he co-signed, re-iterated his concerns and cited the 2 July 2010 memo from MG Flynn. *See* Attachment G.
  - f. Politico chronicled the aforementioned correspondences and, citing multiple former Army intelligence Officers, reported about “the system being prone to crashes and frequently going offline.” *See* Attachment H.
5. On 22 September 2011 DefenseNews reported on DCGS-A system crashes during a joint exercise with South Korea. The article, which employed a senior intelligence official as a source, noted, “[w]hen American intelligence analysts tried to use the software to track simulated North Korean troop movements, the screens on the DCGS-A workstations sometimes went black, forcing them to reboot the software.” *See* Attachment I.
6. At the time of PFC Manning’s deployment the DCGS-A system did not incorporate cloud computing, as such technology was not employed by deployed U.S. Soldiers until November 2010. *See* Attachment A.

## WITNESSES/EVIDENCE

7. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the referenced attachments to this motion in support of its request.

- a. DCGS-A information paper produced by HQDA DCS, G-2 Initiatives Group
- b. DCGS-A Commander's Handbook
- c. Memorandum from MG Michael Flynn to the Deputy Commanding General for Support, USFOR-A, dated 2 July 2010
- d. Letter from Representatives Gabrielle Giffords, Mike McIntyre and Adam Smith to the Honorable Norm Dicks and the Honorable C.W. Young, dated 19 July 2010.
- e. Letter from COL Peter Newell to the Honorable Norm Dicks, dated 28 July 2010.
- f. Letter from Representatives Giffords and Smith to COL Newell, dated 25 August 2010
- g. Letter from Representative Smith to General Martin Dempsey, dated 23 May 2011
- h. "Computer bugs hurt Army ops," by Charles Hoskinson, *Politico*, 29 June 2011
- i. "U.S. Army intel software crashes during exercise," by Ben Iannotta, *DefenseNews*, 22 September 2011.

## LEGAL AUTHORITY AND ARGUMENT

8. In the interest of judicial economy, M.R.E. 201 relieves a proponent from formally proving certain facts that reasonable persons would not dispute. There are two categories of adjudicative facts that may be noticed under the rule. First, the military judge may take judicial notice of adjudicative facts that are "generally known universally, locally, or in the area pertinent to the event." M.R.E. 201(b)(1). Under this category of adjudicative facts, it is not the military judge's knowledge or experience that is controlling. Instead, the test is whether the fact is generally known by those that would have a reason to know the adjudicative fact. *U.S. v. Brown*, 33 M.J. 706 (N.M.C.A 1992). The second category of adjudicative facts are those "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." M.R.E. 201(b)(2). This category of adjudicative facts includes government records, business records, information in almanacs, scientific facts, and well documented reports. *Id. See also, U.S. v. Spann*, 24 M.J. 508 (A.F.C.M.R. 1987). The key requirement for judicial notice under this category is that the source relied upon must be reliable.

9. Under M.R.E. 201(d), a military judge must take judicial notice if the proponent presents the necessary supporting information. In making the determination whether a fact is capable of being judicially noticed, the military judge is not bound by the rules of evidence. 1 STEPHEN A. SALTZBURG, LEE D. SCHINASI, AND DAVID A. SCHLUETER, *MILITARY RULES OF EVIDENCE MANUAL* 201.02[3] (2003). Additionally, the information relied upon by the party requesting judicial notice need not be otherwise admissible. *Id.* The determination of whether a fact is capable of being judicially noticed is a preliminary question for the military judge. *See* M.R.E. 104(a).

10. Here, the inadequacies of the DCGS-A system are readily apparent. At the time PFC Manning was deployed to Iraq he DCGS-A system was prone to frequent crashes and often left users, like PFC Manning disconnected. By mid-2010 these issues were well-known in both military and political circles. In fact, both military and political officials had identified these serious faults with the DCGS-A system and memorialized those faults in correspondence amongst themselves. These correspondences were then reported in the mainstream media and reinforced by intelligence sources that had spent extensive time using the system. It is clear that the inadequacies and issues with the DCGS-A were well known within the military community. Thus, the DCGS-A inadequacies are known "in the area pertinent to the event generally known by those that would have a reason to know the adjudicative fact. As such, it is appropriate to take judicial notice of the DCGS-A inadequacies. M.R.E. 201(b)(1) and *Brown*.

#### CONCLUSION

11. Based on the above, the Defense requests that the Court to take judicial notice of requested adjudicate facts.

Respectfully Submitted



JOSHUA J. TOOMAN  
CPT, JA  
Defense Counsel



# **ATTACHMENT A**

## **Distributed Common Ground System - Army (DCGS-A)**

### **What is it?**

The Distributed Common Ground System - Army (DCGS-A) is the Army's premier intelligence, surveillance, and reconnaissance (ISR) enterprise for the tasking of sensors, analysis and processing of data, exploitation of data, and dissemination of intelligence (TPED) across all echelons. It is the Army component of the larger Defense Intelligence Information Enterprise (DI2E) and interoperable with other Service DCGS programs. Under the DI2E framework, USD (I) hopes to provide COCOM Joint Intelligence Operations Centers (JIOCs) capabilities interoperable with DCGS-A through a Cloud/widget approach. DCGS-A connects tactical, operational, and theater-level commanders to hundreds of intelligence and intelligence-related data sources at all classification levels and allows them to focus efforts of the entire ISR community on their information requirements. This system allows analysts to use a growing menu of advanced analytic tools which enable users to better understand norms, detect change, discern linkages, appreciate significance, cue collection, and identify, track, and target hostile forces in a timely and effective manner. This capability provides analysts the ability to rapidly mine, fuse, and visualize data on top of geospatially-oriented layers to gain unprecedented contextual understanding of their operational environment. DCGS-A provides organizational elements the ability to control select sensor platforms and receive and process the collected data. The enhanced speed, accuracy, and relevance of the ISR effort provides commanders the intelligence information they need, when they need it, to plan and conduct full spectrum operations in counter-insurgency environments and across the full range of military operations.

### **What has the Army done?**

The Army recognized that the counter-insurgency fight is at the BCT, battalion, and company level and yet analysis hardware and software was not fielded below battalion-level. Therefore, in addition to the initial capability set fielded across the force from battalion to Army Service Component Command (ASCC), the Company Intelligence Support Team (CoIST) concept was developed and deploying CoISTs are being equipped with DCGS-A. Additionally, the Army has worked aggressively to incorporate DCGS-A into all combat training centers with a full suite of systems. The DCGS-A provides users access to more than 200 data sources and allows rapid collaboration through shared data access. The system enables tactical analysts the ability to leverage analytical support from National agencies, combatant commands, military intelligence brigades, and tactical Army units in the train/ready phase of Army Force Generation (ARFORGEN). The ability for deploying units to access the same battle space awareness information as their deployed counterparts significantly increases pre-deployment readiness by providing current intelligence products in support of pre-deployment training and operational planning. DCGS-A has incorporated cutting edge technology in the form of cloud computing and advance analytics to provide users with precision search, increased computing speed, enhanced collaboration, and data aggregation tools. The ISR Task Force resourced Program Manager (PM) DCGS-A to

implement this architecture on the SIPRNet in support of deployed operations. The first tactical cloud was deployed to Afghanistan in November 2010 and became operational in March 2011, followed by the CX-I coalition cloud in May 2011. This implementation is the Army's response to a theater Joint Urgent Operational Needs Statement (JUONS) for advanced analytics. The Joint Interoperability Test Command (JITC) completed an assessment of the DCGS-A SIPR Cloud v1.0, with favorable results, in December 2010.

### **What continued efforts does the Army have planned for the future?**

The Army will continue to integrate new technical upgrades into the DCGS-A enterprise and field them in accordance with the ARFORGEN cycle. The program leverages existing government and commercial technologies and integrates them within a common framework to accelerate the delivery of new capabilities. The next version of DCGS-A software will focus on enhancing the geospatial layers and analyst interface, integrate Human Intelligence (HUMINT) tools, and introduce Full Motion Video (FMV) exploitation capabilities and new applications or widgets. Additionally, to enhance the capability to respond to commanders' most computer resource intensive and challenging intelligence questions and scenarios, the Army will introduce cloud edge nodes into the Afghanistan ISR architecture. Recent advances in cloud computing technology have resulted in the development of an edge node capable of extending the cloud architecture and provide advanced analytics capabilities and enhanced storage capacity to remote locations. The PM DCGS-A is postured to begin fielding edge nodes to Afghanistan during 4<sup>th</sup> quarter FY 11, to a limited set of operating bases. Every effort is made to continually expand DCGS-A access to other libraries of data. At the request of units in Iraq and Afghanistan, the Defense Intelligence Agency permitted the ingestion of several of its data sources into the DCGS-A enterprise and the Marine Corps allowed ingestion of their intelligence products via MarineLink. The Department of the Army Intelligence and Information Service and DCGS-A program engineers work daily to identify, access, and ingest new data sources and monitor the transfer of volumes of data across the various network domains.

### **Why is this important to the Army?**

The Army requires relevant, accurate, and timely ISR support to provide commanders the information they need to fight and win counterinsurgency conflicts. DCGS-A is the Army's modern ISR TPED capability that allows commanders from company to ASCC levels to focus the efforts of the entire ISR community - tactical, joint, coalition, and national - on their own information requirements.

As of July 2011  
HQDA DCS, G-2 Initiatives Group (DIG)  
(703) 693-6210  
[dcsg2dig@mi.army.mil](mailto:dcsg2dig@mi.army.mil)

# **ATTACHMENT B**

**COMMANDER'S HANDBOOK  
DISTRIBUTED COMMON GROUND SYSTEM –  
ARMY  
(DCGS-A)**



**FOR OFFICIAL USE ONLY**

**TCM-SP Final Draft  
March 30, 2009**

Distribution authorized to U.S. Government Agencies and their contractors only to protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary (Department of Defense (DoD) Directive 5230.24 Distribution Statements C and D). This determination was made on 31 March 2004. Other requests for this document shall be referred to Department of the Army, Deputy Chief of Staff, G-3, ATTN: DAMO-RQ, 400 Army Pentagon, Washington, DC 20310-0400.

**FOR OFFICIAL USE ONLY**

Commander's Handbook Distributed Common Ground System (DCGS A)

THIS PAGE INTENTIONALLY LEFT BLANK

# FOR OFFICIAL USE ONLY

Commander's Handbook Distributed Common Ground System (DCGS A)

## EXECUTIVE SUMMARY

Access to the Intelligence Enterprise is through the Distributed Common Ground System-Army (DCGS-A). This Commander's Handbook is an overview of the capabilities DCGS-A is providing to the commander. It addresses the benefits of employment of DCGS-A as a whole, rather than any particular fielded version.

DCGS-A, as a component to the DoD Distributed Common Ground/Surface System Mission Area program, is greatly contributing to the Joint and combined Warfighter needs.

DCGS-A enables the Commander to fight in ways that exceed the historical limitations through the following *three interrelated main ideas*:

- 1.) Increased situational awareness reduces risk for the Commander when executing missions.
- 2.) A flattened network enables Commanders greater access to information historically only available to Corps and above echelons.
- 3.) Providing Commanders with unprecedented access to the Intelligence Enterprise affords the greatest impact at the lowest level.

The *three core functionalities* of DCGS-A are:

- 1.) It is the ISR component of Battle Command.
- 2.) It provides analysts a net enabled capability to exploit information with common analyst tools.
- 3.) It receives direct feeds from multiple sensors.

DCGS-A has *three configurations*, which enable Commanders to tailor the system and its components to fit their mission needs:

- 1.) Fixed configuration- Primarily it leverages the power and stability of sanctuary for the most complex processing and analytic tasks, and is currently available.
- 2.) Mobile configuration- Provides tactical, expeditionary, and deployable capabilities to Brigade Command Team (BCT) and other Commanders and is currently a quick reaction capability (QRC).
- 3.) Embedded software- On battle command systems (BCS) enables access to the intelligence enterprise down to the platform (e.g. Future Combat Systems (FCS)).

This handbook is a living document. Updates will follow as the DCGS-A system progresses. This will allow Commanders a concise reference guide to the capabilities provided to their units and its application to leverage DCGS-A against current and future adversaries.

**FOR OFFICIAL USE ONLY**

Commander's Handbook Distributed Common Ground System (DCGS A)

THIS PAGE INTENTIONALLY LEFT BLANK



# FOR OFFICIAL USE ONLY

Commander's Handbook Distributed Common Ground System (DCGS A)

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	iii
<b>Chapter 1 OVERVIEW</b> .....	<b>1 -</b>
1-1. Introduction .....	1 -
1-2. Army Task (ART) List and DCGS-A Application .....	2 -
1-3. Challenges .....	4 -
1-4. Main Idea .....	4 -
<b>Chapter 2 FUNCTIONALITY</b> .....	<b>7 -</b>
2-1. ISR Component of Battle Command .....	7 -
2-2. Common Analyst Tools .....	7 -
2-3. Sensor Injects .....	8 -
<b>Chapter 3 DESCRIPTION</b> .....	<b>9 -</b>
3-1. DCGS-A Configurations .....	9 -
3-2. Where We Are at in Development .....	10 -
<b>Chapter 4 CONCLUSION</b> .....	<b>12 -</b>
4-1. Conclusion .....	12 -

**FOR OFFICIAL USE ONLY**

Commander's Handbook Distributed Common Ground System (DCGS A)

THIS PAGE INTENTIONALLY LEFT BLANK

## FOR OFFICIAL USE ONLY

Commander's Handbook Distributed Common Ground System (DCGS A)

### Chapter 1

#### OVERVIEW

*"My background is that I am an 11B that re-classed to a 25B, now working as an independent company level S2. Considering no formal training other than a two-day familiarization course and that I don't hold an INTEL MOS, I was able to use these DCGS-A tools to create products that my Commanding Officer commented, "I have not seen anything like this below the division level before." I have extensively used a set of tools from DCGS-A: ArcGIS and PSI Jabber. I was able to use ArcGIS to prepare maps using imagery from the server and imagery I imported from Buckeye and WARP. This allowed us to create products rapidly that were not previously practical for a unit at a low level such as ours, and Infantry Companies. Otherwise, we would need to send out RFI's to outside organizations that would not allow the flexibility or time constraints that our mission required. PSI Jabber allowed me to send large files to lower echelon units."*

SGT Charles A. Fair  
S2 C co. 1/279 IN (SEP),  
300th MP BDE, Iraq

#### 1-1. INTRODUCTION

a. As the Intelligence Surveillance and Reconnaissance (ISR) component of Battle Command, DCGS-A provides the Commander faster and more complete situational awareness enabling better understanding of the operational environment. This increased situational awareness allows the Commander to fight in ways that exceed the historical limitations through the following three interrelated main ideas:

- 1.) Increased situational awareness reduces risk for the Commander when executing missions.
- 2.) A flattened network enables Commanders greater access to information historically only available to Corps and above echelons.
- 3.) Providing Commanders with unprecedented access to the Intelligence Enterprise affords the greatest impact at the lowest level.

b. The capabilities of DCGS-A align the center of gravity shift from the division to the BCT with increased accessibility to critical information to fulfill the mission requirements. The accessibility to previously restricted information provides the Commander at the lowest level the capability to leverage the vast intelligence enterprise

## FOR OFFICIAL USE ONLY

Commander's Handbook Distributed Common Ground System (DCGS A)

to better assess the current operational environment and to receive actionable intelligence in a timely manner. Previously, collection, processing, and analysis from a stove-piped process restricted critical information from most Commanders, particularly at brigade and below. Consequently, their decisions, often made without the critical information, came with high risk. DCGS-A reduces that high risk and enables the Commanders to better drive combat operations.

### 1-2. ARMY TASK (ART) LIST AND DCGS-A APPLICATION

a. In conjunction with the three main ideas, DCGS-A, through system configuration and application, enables the Commander to meet seven of his Army Tasks as depicted below through system configuration and application.

1.) ART 1.0: The DCGS-A primary warfighting function is the intelligence warfighting function (IWF). The IWF is the flexible and adjustable activity to generate knowledge of and products portraying the enemy and the environmental features required to plan, prepare, execute, and assess operations. The personnel and organizations within the IWF conduct four primary tasks that facilitate the Commander's visualization and understanding of the threat and the environment. These tasks are interactive and often take place simultaneously throughout the intelligence process. DCGS-A supports the following Army tasks and mission areas:

- a.) ART 1.1: Support to situational understanding (and all sub-tasks).
  - b.) ART 1.2: Support to strategic responsiveness (and all sub-tasks).
  - c.) ART 1.3: Conduct Intelligence, Surveillance and Reconnaissance (and all sub-tasks).
  - d.) ART 1.4: Provide Intelligence Support to Effects (and all sub-tasks).
- b. The IWF also conducts multiple tasks associated with the following non-intelligence discipline warfighting functions:

- 1.) ART 7.2: Manage Tactical Information<sup>1</sup>.
  - a.) Integrate Intelligence Products.
  - b.) Collect Relevant Information.
  - c.) Process Relevant Information to Create a Common Operational Picture.
  - d.) Display a Common Operational Picture (COP) Tailored to user Needs.
  - e.) Store Relevant Information.
  - f.) Disseminate Common Operational Picture and Execution Information to Higher, Lower, Adjacent, supported and Supporting Organizations.
  - g.) Communicate with Non-English Speaking Forces and Agencies.

---

<sup>1</sup> Note: Where it includes the processing of sensor data, the interpretation of data into intelligent information, fusion and integration of separate source data, management of the data to include accuracy and data topology, and dissemination of tactical data information.

## FOR OFFICIAL USE ONLY

Commander's Handbook Distributed Common Ground System (DCGS A)

### 2.) ART 7.3: Assess Tactical Situation and Operations.

- Monitor the Situation or Progress of Operations.
- Evaluate Situation or Operation.
- Provide Combat Assessment.

### 3.) ART 7.4: Plan Tactical Operations Using the Military Decision Making Process/Troop Leading Procedures

- Provide Space support.

c. DCGS-A is the centerpiece of the future Army ISR framework and is the enabler for intelligence functions at the brigade combat team (BCT) and battalion (BN). DCGS-A provides unprecedented access to a wealth of information and sources thereby greatly improving situational awareness. Through Congressional and Under Secretary of Defense (Intelligence) (USD (I)) support, the Army accelerated the development and fielding of DCGS-A. Figure 1-1 graphically illustrates the process in which DCGS-A facilitates the requirements outlined in the AUTL.

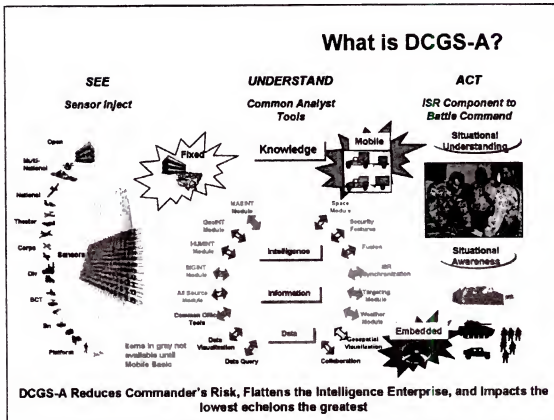


Figure 1-1. What is DCGS-A

## FOR OFFICIAL USE ONLY

Commander's Handbook Distributed Common Ground System (DCGS A)

### 1-3. CHALLENGES

a. Historically, operational focus resided at the division; moreover, the enemy fight was conventional. The programs of record (POR) supported the conventional fight at the cost of irregular warfare. Modularity restructuring, reinforced by Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF), generated focus at the BCT level and below, thereby highlighting shortfalls in current and near term intelligence structures and capabilities. This presented new challenges for the commanders. Now, BCT Commanders are responsible for providing operational focus and actionable intelligence that once came from higher. They must ensure the intelligence is accurate and timely to reduce the risk for mission requirements. The challenge became how to provide the unrestricted access to the BCT Commander. QRC provided the solution through DCGS-A (V2).

b. Secondly, U.S. Forces face adversaries that are highly complex and able to quickly adapt to any given situation. They constantly re-evaluate successes versus failures and adjust their operations for the maximum impact on U.S. and Coalition forces. In addition, adversaries possess the capability to acquire and manipulate various types of networks (e.g. electronic, human) to their advantage. This complicates the adversary's profile and challenges the U.S. forces' ability to predict enemy courses of action (COA). This ability to leverage various networks provides adversaries the advantages of unpredictability.

c. Finally, the enemy's ability to leverage the complexity of urban and provincial domains to their advantage allows them to remain camouflaged to collection resources. This presents an ISR challenge to U.S. and Coalition Forces.

d. DCGS-A allows Commanders to mitigate these diverse challenges with essential capabilities (e.g. leverage more collection quickly and counter threat actions). These capabilities enable Commanders to disrupt the adversary decision cycles and shift the operational advantage back to U.S. Forces. The results, listed below, allow three main ideas to meet the commander's needs through DCGS-A:

- 1.) Reduce Risk to U.S. Forces
- 2.) Flatten Network Communications
- 3.) Greatest Impact felt at the lowest level

### 1-4. MAIN IDEA

a. The Army's transformation from a division centric to a modular, expeditionary, brigade-centric force placed the BCT at the center of current and future combat operations. While operational focus was on the BCT, the level of information access stopped at division.

b. **REDUCE RISK:** DCGS-A reduces or mitigates risk by providing robust access to information that is of greater volume, variety, and fidelity; therefore facilitating precise and timely decision-making. Effective planning reduces uncertainty when informed by accurate intelligence and allows Commanders to mitigate risk presented by the enemy.

## FOR OFFICIAL USE ONLY

Commander's Handbook Distributed Common Ground System (DCGS A)

Essentially, as situational awareness increases, the level of risk decreases. The problem is having access to that information.

c. FLATTENED NETWORK: Historically, brigade and battalion Commanders were slow to receive relevant threat information to execute missions. Often times, requests for information (RFI) were left unanswered due to stove piped congestion. Consequently, this left Commanders to rely on their experience to fill the information gaps before and during their decision cycles. With an evolving, proactive, and highly responsive adversary, this created higher risks. Faced with a versatile adversary, Commanders require direct access to processed intelligence data (i.e., threat warning and locational data), as well as a conduit to receive analyzed information to have the advantage in the operational environment. In addition, Commanders may need to redirect ISR assets to fully assess the operational environment. Timely access to critical combat information and intelligence provides Commanders and Soldiers with detailed situational awareness.

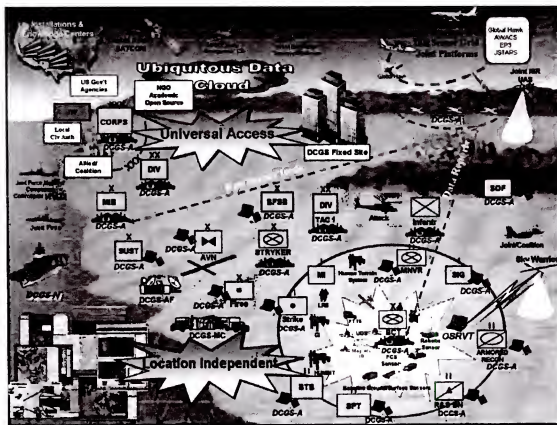
1.) The DCGS-A network enabled structure provides access to the multiple databases and near real time (NRT) direct links from collectors. This access provides an unprecedented conduit to ISR sensors and databases. In addition, this access is not only to Army information but also to Joint, National and Coalition forces' information. The improved access empowers Commanders with NRT intelligence at the lowest command level. This capability sharply enhances the lethality, survivability, agility, versatility, and sustainability of the force and enables more timely and precise application of combat power. For example, intelligence analysts simply take the Commanders RFI and query, using the DCGS-A access to database repositories, for answers that previously were left unanswered.

d. GREATEST IMPACT FELT AT LOWEST LEVEL: Commanders plan missions to obtain the advantage in the operational environment. Previously, restricted information and intelligence limited the knowledge base extendable to the Soldiers executing the missions. Consequently, Soldiers executed missions in a disadvantaged state and walked into many lethal situations that were avoidable with more critical and NRT information available.

1.) DCGS-A provides commanders, including those at BCT and lower levels, an unprecedented access to this critical information, thus extending the flow of information and knowledge down to the Soldier. This enhanced information, knowledge, affords the Soldier to have a greater situational awareness. More importantly, Soldiers lives are saved and risk greatly reduced by this access, because Commanders now can plan the mission down to the most critical probable change in enemy activity.

2.) The Operational View One (OV1) illustrates how DCGS-A incorporates these three main ideas described above in creating a network-enabled capability to the Future Force. DCGS-A allows combat information and intelligence to be available on the same network and linked to the lowest tactical level.

## Commander's Handbook Distributed Common Ground System (DCGS A)



**Figure 1-1. DCGS-A OV-1 and Future Force.**



## **FOR OFFICIAL USE ONLY**

Commander's Handbook Distributed Common Ground System (DCGS A)

### **Chapter 2**

#### **FUNCTIONALITY**

##### **2-1. ISR COMPONENT OF BATTLE COMMAND**

a. DCGS-A is the ISR component of the modular and future force BCS and the Army's primary system for ISR tasking of sensors, processing of data, exploitation of data, and dissemination of intelligence (TPED) information. DCGS-A provides critical battle information about the threat, weather, and terrain at all echelons. DCGS-A will provide the capabilities necessary for Commanders to access information, task organic sensors, and synchronize non-organic sensor assets with their organic assets. These services will be shared by Commanders across an enterprise (provided by the Network-Centric Enterprise Services (NCES)) using the DCGS Integration Backbone (DIB) to enhance interoperability of ISR information.

b. DCGS-A will provide continuous acquisition and synthesis of data and information from Joint, Interagency, Intergovernmental, and Multi-national (JIIM) sources that will permit Commanders to have an updated and accurate picture of the operational environment. This will allow Commanders to maximize their combat power and enhance their ability to operate in an unpredictable and changing environment throughout the operational spectrum.

c. DCGS-A will provide critical accessibility to combat information as the ISR component of Battle Command. By providing a two-way information flow from the BCS to the intelligence enterprise, DCGS-A will enable the intelligence enterprise the accessibility to surveillance and reconnaissance obtained through non-military intelligence collections.

##### **2-2. COMMON ANALYST TOOLS**

a. Providing unrestricted access to intelligence information to the Brigade Commander has always been a challenging process. Historically, the ability to provide critical NRT intelligence took 30 military intelligence vehicles manned with over 100 Soldiers to produce the situational awareness and resided at the division level. The composition of a brigade could not handle such an increase in footprint. However, DCGS-A has reduced this footprint to approximately seven vehicles. By incorporating various programs of record (POR) into one system, this allows Commanders to equip the analyst, instead of manning the equipment. One of the ways this occurs is by reducing duplicate functionality and providing common analyst tools.

b. Formerly, analysts were required to have specialized training on specific operating systems to maximize the full effect of an operational intelligence community. The common tasks of analyzing, mapping, and disseminating finished products were

## FOR OFFICIAL USE ONLY

### Commander's Handbook Distributed Common Ground System (DCGS A)

accomplished in completely different ways. An example of this is the process it would take to provide actionable intelligence to the BCT. The Human Intelligence (HUMINT) collector would input his data into a HUMINT system. He would use his own mapping and analytical tools to produce a product. Analysts would attempt to pass the product through a different communication support system. Unfortunately, his products were not compatible with the All Source Analyst's system and would often be unactionable or lost due to data incompatibility. Unless the All Source Analyst directly spoke to the HUMINT teams, this information was not included in the COP. For example, critical information about the pattern of life or social tendencies was not included in the actionable intelligence and would leave patrols or tactical HUMINT teams (THT) exposed.

c. DCGS-A provides common tools to assist in providing all analysts a greater understanding of each discipline and enables cross training. Common tools enhance analyst's ability to share data and information and to collaborate on answering the Commander's PIR. These tools support a central DCGS-A concept of teaming to solve problem sets vice depending on the current discipline-centric approach. This increases awareness within the operating cell and leads to more precise collection plans, and situational development.

### 2-3. SENSOR INJECTS

a. DCGS-A replaces multiple stove-piped sensor catcher mitts for intelligence, surveillance and reconnaissance with a single ground station capability that is tailorable to the mission. DCGS-A provides a central information point by incorporating various POR into one system allowing for ground base operating stations for sensors to deposit information into one central location.

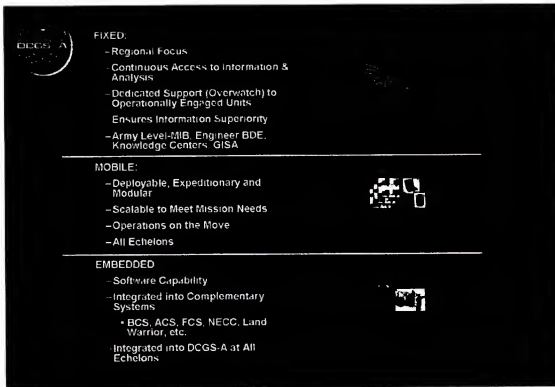
b. While serving as the central inject point DCGS-A also provides the tools for the unique intelligence processing techniques while simultaneously enabling collaboration with other specific intelligence end products. DCGS-A allows for various sensor data injects to be readily crossed referenced with other sources in NRT. Through use of one intelligence system, DCGS-A, Commanders can now equip their analysts at the lower echelons, with common tool sets, without increasing the footprint. Therefore, an unprecedented amount of information and knowledge is available to them. Analysts can provide a more defined operational picture for the Commander and the Commander can quickly identify gaps and redirect the sensors to collect in those areas where his knowledge may be limited.

## Chapter 3

### DESCRIPTION

#### 3-1. DCGS-A CONFIGURATIONS

a. The DCGS-A fielding of various configurations extends across BCT, fires, maneuver enhancement, Battlefield Surveillance Brigade (BFSB), aviation and sustainment organizations. The fixed, mobile, and embedded configurations allow Commanders to have a better awareness and enable understanding of the operational environments in NRT. Figure 3-1 illustrates various configurations.



**Figure 3-1. DCGS-A Configurations**

b. **FIXED:** The fixed configuration leverages the power and stability of sanctuary for the most complex processing and analytic tasks. Additionally, it provides the greatest historical data repository. Aligned geographically, INSCOM Theater Brigades host these fixed sites. Additional sites exist primarily for redundancy and accessibility. The fixed DCGS-A configurations facilitate reach and split-based operations by providing the "heavy lifting" intelligence analysis and strategic planning from stationary locations.

## FOR OFFICIAL USE ONLY

Commander's Handbook Distributed Common Ground System (DCGS A)

Regionally focused, fixed DCGS-A performs a dedicated overwatch function for operationally engaged units. The fixed configuration connects other variations of DCGS System of Systems, and National Sources through provided communications.

c. **MOBILE:** The mobile configuration of DCGS-A provides a tactical, deployable capability to deliver responsive, forward support to Commanders from BN through operational headquarters. Analytical tools, sensor inject, data storage, and integration with other BCS are the highlights of the Mobile configuration. The configuration is the "access" point or intelligence service provider for ISR data and information in theater. DCGS-A via its analysts will provide the Commander with timely and accurate targeting information, intelligence products and predictions on probable enemy COA. Mobile DCGS-A provides a wide range of ISR capabilities including direct downlink of select DCGS baseline sensors, robust tasking, posting, processing, using (TPPU) tools, and advance ISR analysis capabilities directly support tactical and force protection operations. Mobile DCGS-A is scalable and tailorable based on mission, enemy, terrain and weather, troops, time available and civilian considerations (METT-TC). Lastly, DCGS-A Mobile has the capability of receiving "plug" augmentation for increased capability while remaining connected to various networks through provided communications.

d. **EMBEDDED:** The embedded DCGS-A software on BCS enables the connection of the intelligence enterprise with the battle command network (e.g. FCS). Embedded software provides battalion and company intelligence efforts unprecedented access to data never before available. Historically, surveillance and reconnaissance collected from non military intelligence sources was not available to the intelligence enterprise. The embedded software provides the shared access to both battle command and the intelligence enterprise. This ability enables a more complete picture of the operational environment to the commander. Embedded software capabilities provide commonality and standardization to improve interoperability, reduce training time, and increase sustainability across the Future Force. It resides on local workstations and is available through the network. The network secures the embedded software through user access and permissions.

### 3-2. WHERE WE ARE AT IN DEVELOPMENT

a. DCGS-A follows an evolutionary acquisition strategy to develop and field capability incrementally throughout its life cycle.

1.) The initial DCGS-A effort improved on interoperability between current force systems and related modifications to POR. Initial DCGS-A efforts also included the integration of the Joint Intelligence Operations Capability-Iraq (JIOC-I) QRC. This product, renamed DCGS-A Version 2 (V2), was fielded to OIF/OEF units in FY 06-07 and provided access to over 200 data sources. The next DCGS-A step was the development and fielding of Version 3.0 hardware and software, which added the DCGS Integration Backbone (DIB) as well as two-way Battle Command interoperability. DCGS-A Version 3.1 (V3.1) adds Joint interfaces, will be fielded worldwide beginning in FY 09, and will displace ASAS-Light. The initial DCGS-A effort also included

## **FOR OFFICIAL USE ONLY**

Commander's Handbook Distributed Common Ground System (DCGS A)

standing up a fixed facility capability at each of the Army Military Intelligence Brigades (MIB).

2.) The current DCGS-A effort develops, produces and fields a DCGS-A Mobile (vehicle mounted and deployable) capability in two increments: the Mobile Basic and the Mobile Extended. The Army's rationale for separating the developmental efforts is to provide a mobile BCT focused capability to the force as early as possible while reducing risk associated with achieving specific attributes where technology readiness levels (TRL) would delay fielding of the capability of the Force.

3.) The follow-on DCGS-A Mobile Extended effort will integrate capabilities provided by other Office of the Secretary of Defense (OSD) programs, will provide the embedded ISR capability to Army Battle Command and FCS; the ground station capability for the Aerial Common Sensor; and a DCGS-A capability throughout the force. The Army anticipates a milestone B decision for the DCGS-A Mobile Extended in FY12.

## INSTRUCTIONS FOR PREPARING AND ARRANGING RECORD OF TRIAL

**USE OF FORM** - Use this form and MCM, 1984, Appendix 14, will be used by the trial counsel and the reporter as a guide to the preparation of the record of trial in general and special court-martial cases in which a verbatim record is prepared. Air Force uses this form and departmental instructions as a guide to the preparation of the record of trial in general and special court-martial cases in which a summarized record is authorized.

Army and Navy use DD Form 491 for records of trial in general and special court-martial cases in which a summarized record is authorized. Inapplicable words of the printed text will be deleted.

**COPIES** - See MCM, 1984, RCM 1103(g). The convening authority may direct the preparation of additional copies.

**ARRANGEMENT** - When forwarded to the appropriate Judge Advocate General or for judge advocate review pursuant to Article 64(a), the record will be arranged and bound with allied papers in the sequence indicated below. Trial counsel is responsible for arranging the record as indicated, except that items 6, 7, and 15e will be inserted by the convening or reviewing authority, as appropriate, and items 10 and 14 will be inserted by either trial counsel or the convening or reviewing authority, whichever has custody of them.

1. Front cover and inside front cover (chronology sheet) of DD Form 490.
2. Judge advocate's review pursuant to Article 64(a), if any.
3. Request of accused for appellate defense counsel, or waiver/withdrawal of appellate rights, if applicable.
4. Briefs of counsel submitted after trial, if any (Article 38(c)).
5. DD Form 494, "Court-Martial Data Sheet."
6. Court-martial orders promulgating the result of trial as to each accused, in 10 copies when the record is verbatim and in 4 copies when it is summarized.
7. When required, signed recommendation of staff judge advocate or legal officer, in duplicate, together with all clemency papers, including clemency recommendations by court members.

8. Matters submitted by the accused pursuant to Article 60 (MCM, 1984, RCM 1105).

9. DD Form 458, "Charge Sheet" (unless included at the point of arraignment in the record).

10. Congressional inquiries and replies, if any.

11. DD Form 457, "Investigating Officer's Report," pursuant to Article 32, if such investigation was conducted, followed by any other papers which accompanied the charges when referred for trial, unless included in the record of trial proper.

12. Advice of staff judge advocate or legal officer, when prepared pursuant to Article 34 or otherwise.

13. Requests by counsel and action of the convening authority taken thereon (e.g., requests concerning delay, witnesses and depositions).

14. Records of former trials.

15. Record of trial in the following order:

- a. Errata sheet, if any.
- b. Index sheet with reverse side containing receipt of accused or defense counsel for copy of record or certificate in lieu of receipt.
- c. Record of proceedings in court, including Article 39(a) sessions, if any.
- d. Authentication sheet, followed by certificate of correction, if any.
- e. Action of convening authority and, if appropriate, action of officer exercising general court-martial jurisdiction.
- f. Exhibits admitted in evidence.
- g. Exhibits not received in evidence. The page of the record of trial where each exhibit was offered and rejected will be noted on the front of each exhibit.
- h. Appellate exhibits, such as proposed instructions, written offers of proof or preliminary evidence (real or documentary), and briefs of counsel submitted at trial.